UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: ALL CASES	MDL No. 1:23-md-03083-ADB-PGL

PLAINTIFFS' BELLWETHER CONSOLIDATED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

PREAMBLE

The following Plaintiffs allege as set forth herein:

- "**Maximus Bellwether Plaintiffs**": Gregory Bloch, Barbara Cruciata, Benjamin Dieck, Victor Diluigi, S.K. and M.K. (minors through their legal guardian), Shellie Harper McCaskell, Elaine McCoy, Robert Plotke, Jvanne Rhodes, M.P. and M.Y. (minors through their legal guardian), and Alexys Taylor;
- "**Welltok Bellwether Plaintiffs**": Tamara Williams, Jeffrey Weaver, Amanda Copans, Denise Meyer, Christopher Rehm, Sherrie Rodda, Laquesha George, and Megan McClendon;
- "**Delta Dental Bellwether Plaintiffs**": Karen Boginski, Doris Cadet, Marvin Dovberg, Deanna Duarte, Michelle Gonsalves, Margaret Kavanagh, John Meeks, Terrill Mendler, Manuel Mendoza, Ricardo Moralez, Hannah Polikowsky, Diamond Roberts, Taneisha Robertson, and Yvette Tillman; and
- "**PBI Bellwether Plaintiffs**": Keith Bailey, Camille Burgan, Eugene Burgan, Steven Checchia, Gilbert Hale, Lynda Hale, Brinitha Harris, Patrice Hauser, Tricia Hernandez, Patricia Marshall, Rita Pasquarelli, Margaret Phelan, Jose Soto, Steven Teppler, and Katharine Uhrich.

Collectively, the (a) Welltok Bellwether Plaintiffs, (b) Maximus Bellwether Plaintiffs, (c) Delta Dental Bellwether Plaintiffs, and (d) PBI Bellwether Plaintiffs (i.e., all Plaintiffs named in this Bellwether Consolidated Amended Complaint) shall hereinafter be referred to as the "Bellwether Plaintiffs" or "Plaintiffs."

Pursuant ECF No. 1267—granting Plaintiffs' request to file a single consolidated amended complaint—the instant Bellwether Consolidated Amended Complaint is organized "like chapters in a book, with allegations as to each bellwether defendant set forth in its own section"[1] as follows:

- CHAPTER ONE: Factual allegations concerning all Defendants.
- CHAPTER TWO: Progress Bellwether Chapter
- CHAPTER THREE: PBI Bellwether Chapter
- CHAPTER FOUR: Delta Dental Bellwether Chapter
- CHAPTER FIVE: Maximus Bellwether Chapter
- CHAPTER SIX: Welltok Bellwether Chapter

In **Chapter Two – the Progress Chapter**, all Bellwether Plaintiffs, individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to themselves, bring causes of action and additional allegations against Progress Software Corporation and Ipswitch, Inc. (collectively, "Progress").

In **Chapter Three – the PBI Chapter**, PBI Bellwether Plaintiffs, individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to themselves, bring causes of action and additional allegations against the following Bellwether Defendants, who are collectively referred to hereinafter as the "**PBI Bellwether Defendants**": Genworth Life and Annuity Insurance Company ("GLAIC"), Genworth Life Insurance Company ("GLIC"), Genworth Financial, Inc. ("Genworth Financial" and collectively with GLAIC and GLIC, "Genworth Defendants" or "Genworth"), Milliman Inc. (d/b/a Milliman Intelliscript, Inc.), Milliman Solutions, LLC ("Milliman Solutions" and collectively with Milliman Inc., "Milliman

[1] *See id*. at 5; *see also* ECF No. 1269, 99:22 – 100:4 (Hon. District Judge Allison D. Burroughs: "If you could set it up sort of like chapters in a book ….").

Defendants" or "Milliman"), MEMBERS Life Insurance Company ("MLIC"), Pension Benefit Information LLC d/b/a PBI Research Services ("PBI"), and Teachers Insurance and Annuity Association of America ("TIAA").

In **Chapter Four – the Delta Dental Chapter**, Delta Dental Bellwether Plaintiffs, individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to themselves, bring causes of action and additional allegations against the following Bellwether Defendants, who are collectively referred to hereinafter as the "**Delta Dental Defendants**": Delta Dental of California ("DDCA"), Delta Dental Insurance Company ("DDIC"), Delta Dental of New York ("DDNY"), and Delta Dental of Pennsylvania ("DDPenn") (collectively, "DDCA and Affiliates"), and Delta Dental Plans Association ("DDA") (collectively, with DDCA and Affiliates, the "Delta Dental Bellwether Defendants").

In **Chapter Five – the Maximus Chapter**, Maximus Bellwether Plaintiffs, individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to themselves, bring causes of action and additional allegations against the following Bellwether Defendants, who are collectively referred to hereinafter as the "**Maximus Bellwether Defendants**" or "**Maximus**": Maximus, Inc. ("Maximus Inc."), Maximus Federal Services, Inc. ("MFSI"), Maximus Human Services, Inc. ("MSI"), Maximus Health Services, Inc. ("MHSI").

In **Chapter Six – the Welltok Chapter**, Welltok Bellwether Plaintiffs, individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to themselves, bring causes of action and additional allegations against the following Bellwether Defendants, who are collectively referred to hereinafter as the "**Welltok Bellwether Defendants**": Welltok, Inc. ("Welltok"), Sutter Health ("Sutter Health"), OSF Healthcare System ("OSF"), Corewell Health ("Corewell" or "Corewell Health"), Virginia Mason Franciscan Health ("Virginia

Mason"), CHI Health – NE ("CHI"), and Baylor Scott & White Health ("Baylor Scott")[2] (collectively, Baylor Scott, Corewell, Sutter Health, OSF, CHI, and Virginia Mason are the "Welltok VCE Defendants") (and together Welltok, the Welltok VCE Defendants are the "Welltok Bellwether Defendants").

Progress, PBI Bellwether Defendants, Delta Dental Bellwether Defendants, Maximus Bellwether Defendants, and Welltok Bellwether Defendants (i.e., all Defendants named in this complaint) are hereinafter collectively referred to as "Defendants" or "Bellwether Defendants."

Plaintiffs allege as follows:

I. INTRODUCTION

1. Plaintiffs bring this Bellwether Consolidated Class Action Complaint against Defendants on behalf of themselves and all other similarly situated individuals, stemming from a data breach impacting more than 85 million people,[3] who had their highly sensitive personally identifiable information ("PII")—including, but not limited to, their full names, dates of birth, and Social Security numbers—and protected health information ("PHI," and together with PII, "Private Information") accessed, compromised, and obtained by malicious, unauthorized third parties from Defendants' systems as early as May 27, 2023[4] (the "Data Breach").

[2] The Parties submitted a Joint Submission Regarding Addition of Three Bellwether Parties on November 27, 2024 (ECF 1287), setting out, *inter alia*, their respective positions on the inclusion of Baylor Scott as a bellwether defendant. The Court had not yet ruled on the issue of Baylor Scott's inclusion at the time of the finalization and filing of this Complaint. Should the Court rule that Baylor Scott may not be included as a bellwether defendant at this time, Plaintiffs will remove Baylor Scott and re-file their Bellwether Consolidated Class Action Complaint as soon as possible.

[3] Bert Kondruss, *MOVEit hack victim list*, Kon Briefing, https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html (last updated Dec. 20, 2023).

[4] *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)*, Progress: Community (June 16, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023; Nader Zaveri et al., *Zero-Day Vulnerability in MOVEit Transfer*

2. Defendants tout the safety and security of their services and systems on their websites, particularly their data privacy practices, but failed to adhere to those promises and, instead, allowed the Data Breach to occur.

3. For instance, Progress states: "The security of our customers' environments is paramount. Progress has a comprehensive cybersecurity program in place which includes a zero-trust cybersecurity architecture approach, compliance audits and verifications, source-code scanning, external penetration tests, third-party deep-dive code assessments as well as ongoing coordination with some of the industry's top cybersecurity researchers."[5]

4. Likewise, as alleged in greater detail below, all other Bellwether Defendants make similar statements to consumers that the Personal Information that they entrust to Defendants will remain safe and secure.

5. At the center of the Data Breach, and all Plaintiffs' claims herein, is Progress's on-premises secure file transfer software, MOVEit Transfer, which is represented as providing a "secure environment for your file transfers to help you meet cybersecurity standards, exchange data efficiently, and protect your reputation."[6]

6. MOVEit Transfer is part of Progress's MOVEit suite of products, originally developed by Progress's wholly-owned subsidiary, Ipswitch, Inc. ("Ipswitch"), which Progress acquired in 2019.[7]

Exploited for Data Theft, Mandiant: Blog (Apr. 3, 2024), https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft.

[5] *Progress Trust Center*, Progress: MOVEit, https://www.progress.com/security (last visited Nov. 26, 2024).

[6] *MOVEit: Managed File Transfer Software*, Progress, https://www.progress.com/moveit/moveit-transfer (last visited Dec. 5, 2024).

[7] Larry Dignan, *Progress acquires Ipswitch for $225 million, tops first quarter targets*, ZDNet (Mar. 28, 2019), https://www.zdnet.com/article/progress-acquires-ipswitch-for-225-million-tops-

7. Progress boasts MOVEit as the "leading secure Managed File Transfer (MFT) software used by thousands of organizations around the world to provide complete visibility and control over file transfer activities. Whether deployed as-a-Service, in the Cloud, or on premises, MOVEit enables your organization to meet compliance standards, easily ensure the reliability of core business processes, and secure the transfer of sensitive data between partners, customers, users and systems."[8]

8. Progress' website further assures MOVEit users that it has substantial data privacy protections and practices in place to keep sensitive Private Information secure. For example:

> Progress MOVEit helps your organization meet cybersecurity compliance standards such as PCI-DSS, HIPAA, GDPR, SOC2 and more. Provide a more secure environment for your most sensitive files, while supporting the reliability of core business processes.
>
> * * *
>
> The security of our customers' environments is paramount. Progress has a comprehensive cybersecurity program in place which includes a zero-trust cybersecurity architecture approach, compliance audits and verifications, source-code scanning, external penetration tests, third-party deep-dive code assessments as well as ongoing coordination with some of the industry's top cybersecurity researchers
>
> When vulnerabilities are found, we work quickly to mitigate the risk, issue appropriate patches and communicate directly with our customers, so they can take immediate action to harden their environments against those vulnerabilities.[9]

---

first-quarter-targets/; *Progress Completes Acquisition of Ipswitch, Inc.*, Progress: Press Release (May 1, 2019), https://investors.progress.com/news-releases/news-release-details/progress-completes-acquisition-ipswitch-inc#.

[8] *Managed File Transfer Software*, Progress: MOVEit, https://www.ipswitch.com/moveit (last visited Nov. 26, 2024).

[9] *Progress Trust Center*, Progress: MOVEit , https://www.progress.com/security (last visited Nov. 26, 2024).

9. MOVEit Transfer is software that is licensed to customers on a subscription basis and installed by customers on their own servers, providing the customers with the ability to store, send, and receive sensitive files.[10] MOVEit Transfer is typically accessed by each customer's users through a public-facing web portal that is run on the customer's servers, not Progress's servers.[11]

10. Progress claims MOVEit Transfer encrypts files both in transit and at rest so they cannot be viewed at any time without the appropriate encryption key.[12]

11. In addition to Progress, the other Defendants in this case are customers who contract directly with Progress to use MOVEit Transfer on their own servers, or other vendors who contract with a third party which in turn uses MOVEit Transfer. A variety of parties—such as direct users or vendors—thus used MOVEit software to effectuate file transfers. *See* Exhibit A (Updated Defendant Track Appendix A).

12. Progress' website states that "in some cases, end users of our customers may need to provide Sensitive [Private] Information to our customer in order to make use of an application that uses our Product or SaaS Product and that Sensitive Personal Information may be stored or processed by us as a result. We process such Sensitive [Private] Information in the role of a processor on behalf of a customer (and/or its affiliates) who is the responsible controller of the Sensitive [Private] Information concerned."[13]

---

[10] *More Secure Managed File Transfer Software for the Enterprise*, Progress: MOVEit, https://www.progress.com/moveit/moveit-transfer (last visited Nov. 26, 2024).

[11] *Advanced Topics: Systems Internal – URL Crafting, MOVEit Transfer 2023.1 Adm'r Guide*, Progress: Prod. Documentation (Apr. 21, 2022), https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/System-Internals-URL-Crafting.html.

[12] *Introduction, MOVEit Transfer 2023.1 Adm'r Guide*, Progress: Prod. Documentation (Apr. 21, 2022), https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/Introduction\.html.

[13] https://www.progress.com/legal/privacy-policy.

13. On or around May 31, 2023, Progress discovered a vulnerability in MOVEit Transfer that "could lead to escalated privileges and potential unauthorized access." On or about that same day, Progress purportedly notified all of its customers that used MOVEit (such as Bellwether Defendants), and developed and released a security patch for the vulnerability used in the Data Breach.[14] The vulnerability was given a severity rating under the Common Vulnerability Scoring System of 9.8 out of 10, signifying that the vulnerability is near the highest level of severity, or "critical."[15] As described below, Progress continued to find additional security vulnerabilities in the MOVEit Transfer software as well as its other products.

14. On or around May 27, 2023, the Russian cybercriminal ransomware gang Cl0p exploited MOVEit Transfer's vulnerabilities by simultaneously deploying malware to public-facing MOVEit Transfer web portals of thousands of MOVEit Transfer customers, decrypting the stored data, and downloading it in bulk.[16]

15. Because the MOVEit Transfer software was not designed to discover or defend against this type of attack, it initially went undetected.[17] Further, because MOVEit Transfer is

[14] *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)*, Progress: Community (June 16, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023.

[15] NIST, *Progress MOVEit Transfer SQL Injection Vulnerability (CVE-2023-34362) Detail*, Nat'l Vulnerability Database (June 23, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-34362.

[16] Nader Zaveri et al., *Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft*, Mandiant: Blog (Apr. 3, 2024), https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft.

[17] Nader Zaveri et al., *Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft*, Mandiant: Blog (Apr. 3, 2024), https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft.

installed on each customer's servers, there could be no coordinated effort to stop the attack until Progress published a patch.[18]

16. Cl0p's coordinated attack provided it with unfettered access to unencrypted Private Information of millions of individuals.

17. On June 6, 2023, after the Data Breach was publicized and a patch was rolled out, Cl0p claimed credit for the Data Breach and threatened to post stolen data online unless the compromised organizations paid a ransom.[19]

18. When the deadline expired, Cl0p proceeded to publish terabytes of stolen data on the dark web.[20]

19. By December 20, 2023, over 2,600 organizations—accounting for at least 85 million individual victims—had been compromised in the Data Breach.[21]

20. Despite the immediate notification of Progress's customers about the Data Breach, individual victims, including Plaintiffs, were not notified that their Private Information was compromised until months later.

21. The Private Information of millions of individuals compromised in the Data Breach continues to be circulated on the dark web and leveraged by cybercriminals. In one example, a person or group known as Nam3L3ss has sought to download, clean, and organize all data stolen

[18] Joe Slowik, *Move It on Over: Reflecting on the MOVEit Exploitation*, Huntress: Blog (Jul. 7, 2023), https://www.huntress.com/blog/move-it-on-over-reflecting-on-the-moveit-exploitation.

[19] Nader Zaveri et al., *Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft*, Mandiant: Blog (Apr. 3, 2024), https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft.

[20] Riam Kim-Mcleod, *Clop Leaks: First Wave of Victims Named*, ReliaQuest: Blog (July 28, 2023, 10:00 AM), https://www.reliaquest.com/blog/clop-leaks-first-victims/.

[21] Bert Kondruss, *MOVEit hack victim list*, Kon Briefing, https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html (last updated Dec. 20, 2023).

in the Data Breach to make it easily accessible to cybercriminals, and has already done so with millions of records from dozens of organizations so far.[22] Accordingly, Plaintiffs and individual victims of the Data Breach will continue to be victimized as information obtained from the Data Breach will continue to proliferate on the dark web.[23] And as more information continues to be disclosed by cybercriminals, fraud and attempted fraud and identity theft will continue to occur for millions more individuals.

22. Each and every Defendant was responsible for the collection, storage, and protection of Plaintiffs and Class members' Private Information. Defendants owed duties to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their Private Information against unauthorized access and disclosure. Defendants breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the Private Information entrusted to them from unauthorized access and disclosure, failing to ensure that third-party software followed industry standards for data security, and failing to ensure that third-party vendors used software that followed industry standards for data security, thereby allowing the Data Breach to occur.

[22] Ernestas Naprys, *MOVEit fallout: hackers leak employee data from Amazon, MetLife, HSBC, and other major companies*, cybernews (Nov. 11, 2024, 4:09 PM), https://cybernews.com/security/moveit-fallout-hackers-leak-employee-data-from-amazon-metlife/; Ionut Arghire, *760,000 Employee Records from Several Major Firms Leaked Online*, SecurityWeek (Dec. 3, 2024), https://www.securityweek.com/760000-employee-records-from-several-major-firms-leaked-online/.

[23] Alex Scroxton, *More data stolen in 2023 MOVEit attacks comes to light*, ComputerWeekly.com (Nov. 12, 2024, 4:10 PM), https://www.computerweekly.com/news/366615522/More-data-stolen-in-2023-MOVEit-attacks-comes-to-light. ("Kevin Robertson, chief operating officer at Acumen Cyber, said: "This leak shows how data makes its way across the dark web, often reappearing in the news long after breaches took place and often in the hands of other attackers.").

23. As a result of Defendants' inadequate data security and breach of their duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' Private Information was accessed by, and disclosed to, unauthorized and malicious third-party actors. This instant action seeks to remedy Defendants' failings and their consequences. Plaintiffs thus bring this Complaint on behalf of themselves, and all similarly situated individuals whose Private Information was exposed as a result of the Data Breach, which Progress publicly disclosed on May 31, 2023.

PARTIES

II. PLAINTIFFS

A. Maximus Bellwether Plaintiffs

1. Plaintiff Gregory Bloch

24. Plaintiff Gregory Bloch ("Plaintiff Bloch") is, and was at all relevant times, an individual and citizen of Fleming Island, Florida.

25. Plaintiff Bloch's children received healthcare services through the Florida Healthy Kids Corporation.

26. Plaintiff Bloch received a letter from Maximus, Inc. dated August 25, 2023, that informed him of "an incident that may have involved your personal health information. Maximus provides administrative services to the Florida Healthy Kids Corporation (Healthy Kids) to support its health insurance program. Maximus uses a software called MOVEit Transfer, a third-party software application provided Progress Software Corporation (Progress). The incident involved a critical vulnerability in MOVEit Transfer."

27. The letter states further as follows:

> **What happened?**
>
> On May 30, 2023, Maximus detected unusual activity in our MOVEit environment. We promptly began to investigate with the help of nationally recognized cybersecurity experts. On May 31, 2023, Maximus took our MOVEit application

> offline. Later that same day, Progress first publicly announced a problem with its MOVEit software, which allowed an unauthorized person to gain access to files of many MOVEit customers, including Maximus. ***
>
> Maximus promptly informed Healthy Kids of the incident and we have been working with them since. Additionally, we engaged a forensic investigation firm and a data analysis firm to identify affected individuals and the types of information involved. We learned that on approximately May 27 - May 31, 2023, the unauthorized person obtained copies of certain files that were saved in the Maximus MOVEit application. We then began to analyze the files to determine which data was affected and on June 12, 2023, determined filed related to Healthy Kids were impacted. Our investigation determined that the files contained some of your family's personal information.
>
> **What information Was involved?**
> Although the information impacted by the incident varied by individual, the information involved may include:
> - Name, address, date of birth, phone number, email address
> - Social Security number, other government-issued identifier
> - Tribal identification or enrollment number
> - Family Account Number

28. At the time that Progress discovered the Data Breach—on or around May 31, 2023—Defendants Progress and Maximus, Inc. retained Plaintiff Bloch's PII in their computer systems.

29. Accordingly, the letter states that Progress and Maximus, Inc. possessed Plaintiff Bloch's PII, including his name, address, date of birth, phone number, email address, Social Security number, other government-issued identifier, Tribal identification or enrollment number, and Family Account Number, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

30. According to the letter, Progress and Maximus, Inc. learned of the Data Breach as early as May 30-31, but they waited approximately three months before only Maximus, Inc. notified Plaintiff Bloch that his highly sensitive PII was compromised in the Data Breach.

31. In addition to their substantial delay in notifying Plaintiff Bloch of the Data Breach, Defendants also put the burden on Plaintiff Bloch to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant by reviewing your financial statements and accounts for signs of suspicious transactions and activities. Report any indications of suspected fraud or identify theft to local law enforcement, your State's Attorney General's office, or the Federal Trade Commission."

32. According to the letter, Defendants waited three months before they notified Plaintiff Bloch that his Personal Information was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Bloch, who retains a vested interest in ensuring that his PII remains protected.

33. Moreover, Defendants' disclosure amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Bloch of the Data Breach's critical facts. Without those details, Plaintiff Bloch's ability to mitigate harms resulting from the Data Breach is severely diminished.

34. Plaintiff Bloch's PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. More specifically, Plaintiff Bloch incurred fraudulent charges on his Navy Federal Credi Union debit card in June 2023, which caused him to cancel the card. Additionally, Mr. Bloch was informed by Dark Web Alerts on April 12, 2024 and September 11, 2024 that his Social Security number was compromised. Further, at the direction of Maximus, Inc., Plaintiff Bloch made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, monitoring his accounts for suspicious activity, investigating suspicious activity, and contacting banks, credit card companies,

and other businesses about suspicious activity. Plaintiff Bloch has spent significant time dealing with the Data Breach—valuable time Plaintiff Bloch otherwise would have put to profitable use, including, but not limited to, work and/or recreation. All told, Plaintiff Bloch estimates that he has spent approximately 60 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

35. The Data Breach has caused Plaintiff Bloch fear, anxiety, sleep disruption, stress, anger, fear for his personal financial security, and fear for what information was revealed in the Data Breach, which has been compounded by Defendants' 3-month delay in informing him of the fact that his PII, including his Social Security number, was acquired by known cybercriminals through the Data Breach.

36. Plaintiff Bloch has also experienced a large uptick in fraudulent spam and phishing calls and emails since the Data Breach.

37. Plaintiff Bloch greatly values his privacy and PII and takes reasonable steps to maintain the confidentiality of his PII, including maintaining strong passwords, regularly changing passwords, using multi-factor authentication, promptly investigating any alerts about login attempts or suspicious activity, never engaging in transactions/interacting with businesses he doesn't trust and/or non-reputable vendors, using free identity theft/credit monitoring services; routinely checking same, regularly reviewing financial and other important account activity, storing important documents in a safe place, never transmitting his Social Security number to unknown/untrusted individuals/entities, and shredding/destroying sensitive documents

38. Plaintiff Bloch anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Bloch

will continue to be at present and continued increased risk of identity theft and fraud for years to come.

39. Plaintiff Bloch has a continuing interest in ensuring that his PII, which remains in Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

40. As a result of the Data Breach, Plaintiff Bloch has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of his stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft, time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct, time and expenses spent monitoring bank accounts for fraudulent activity, loss in value of his personal data, lost property in the form of his compromised PII, and injury to his privacy. Additionally, as a direct result of the Data Breach, Plaintiff Bloch now faces a substantial risk that unauthorized third parties will further misuse his PII because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Personal Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of Personal Information CL0P exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Bloch has (1) suffered, or is at an increased risk of suffering, unauthorized use of his stolen PII such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm

because he lost time that he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort he expended addressing future consequences of the Data Breach.

41. Plaintiff Bloch experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Bloch would compensate him for the foregoing redressable injuries. Further, Plaintiff Bloch seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of his PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

2. Plaintiff Barbara Cruciata

42. Plaintiff Barbara Cruciata ("Plaintiff Cruciata") was at all relevant times an individual and citizen of the Bronx, New York, but is now a citizen of Florida, residing in Delray Beach, Palm Beach County as of July 23, 2024.

43. Plaintiff Cruciata has received healthcare services from Medicare through the Centers for Medicare & Medicaid Services.

44. Plaintiff Cruciata received a letter from Maximus Federal Services, Inc. and the Centers for Medicare & Medicaid Services (CMS) dated July 28, 2023, that informed her of "an incident involving your personal information related to services provided by Maximus. The incident involved a security vulnerability in the MOVEit software, a third-party application which allows for the transfer of files during the Medicare appeals process."

45. The letter states further as follows:

> **What Happened?** On May 30, 2023, Maximus detected unusual activity in its MOVEit application. Maximus began to investigate and stopped all use of the MOVEit application early on May 31, 2023. Later that same day, the third-party

application provider, Progress Software Corporation, announced that a vulnerability in its MOVEit software had allowed an unauthorized party to gain access to files across many organizations in both the government and private sectors. Maximus notified CMS of the incident on June 2, 2023. To date, the ongoing investigation indicates that on approximately May 27 through May 31, 2023, the unauthorized party obtained copies of files that were saved in the Maximus MOVEit application, but that no CMS system has been compromised. As part of that analysis, it was determined that those files contained some of your personal information.

What Information Was Involved? We have determined that your personal and Medicare information was involved in this incident. This information may have included the following:

- Name
- Social Security Numbers or Individual Taxpayer Identification Number
- Date of Birth
- Mailing Address
- Telephone Number, Fax number, and Email Address
- Medicare Beneficiary Identifier (MBI) or Health Insurance Claim Number (HICN)
- Driver's License Number and State Identification Number
- Medical history/ Notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.)
- Healthcare Provider and Prescription Information
- Health Insurance Claims and Policy/Subscriber Information
- Health Benefits & Enrollment Information.

46. At the time that Progress discovered the data breach—on or around May 31, 2023—Defendants Progress and Maximus Federal Services, Inc. retained Plaintiff Cruciata's PHI and PII in their computer systems.

47. Accordingly, the letter states that Progress and Maximus Federal Services, Inc. possessed Plaintiff Cruciata's PHI and PII, including her Name, Social Security Numbers or Individual Taxpayer Identification Number, Date of Birth, Mailing Address, Telephone Number, Fax number, and Email Address, Medicare Beneficiary Identifier (MBI) or Health Insurance Claim Number (HICN), Driver's License Number and State Identification Number, Medical history/ Notes (including medical record/account numbers, conditions, diagnoses, dates of service, images,

treatments, etc.), Healthcare Provider and Prescription Information, Health Insurance Claims and Policy/Subscriber Information, and Health Benefits & Enrollment Information, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

48. According to the letter, Progress and Maximus Federal Services, Inc. learned of the Data Breach as early as May 30-31, but they waited approximately two months before only Maximus Federal Services, Inc. notified Plaintiff Cruciata that her highly sensitive PHI and PII was compromised in the Data Breach.

49. In addition to their substantial delay in notifying Plaintiff Cruciata of the Data Breach, Defendants also put the burden on Plaintiff Cruciata to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant by reviewing your financial statements and accounts for signs of suspicious transactions and activities. Report any indications of suspected fraud or identify theft to local law enforcement, your State's Attorney General's office, or the Federal Trade Commission."

50. According to the letter, Defendants waited two months before they notified Plaintiff Cruciata that her Personal Information was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Cruciata, who retains a vested interest in ensuring that her PHI and PII remains protected.

51. Moreover, Defendants' disclosure amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Cruciata of the Data Breach's critical facts. Without those details, Plaintiff Cruciata's ability to mitigate harms resulting from the Data Breach is severely diminished.

52. At the direction of Maximus Federal Services, Inc., Plaintiff Cruciata made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, monitoring her accounts for suspicious activity, and contacting banks, credit card companies, or other vendors about fraudulent/suspicious activity. Plaintiff Cruciata has spent significant time dealing with the Data Breach—valuable time Plaintiff Cruciata otherwise would have put to profitable use, including, but not limited to, work and/or recreation. All told, Plaintiff Cruciata estimates that she has spent approximately 30 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

53. The Data Breach has caused Plaintiff Cruciata fear, anxiety, stress, sleep disruption, anger, headaches, fear for her personal financial security, and fear for what information was revealed in the data breach, which has been compounded by Defendants' 2-month delay in informing her of the fact that her PHI and PII, including her Social Security number, was acquired by known cybercriminals through the Data Breach.

54. Plaintiff Cruciata also experienced a large uptick in fraudulent spam and phishing calls and emails immediately after the Data Breach.

55. Plaintiff Cruciata greatly values her privacy and PHI and PII and takes reasonable steps to maintain the confidentiality of her PHI and PII, including maintaining strong passwords, using multi-factor authentication, promptly investigating any alerts about login attempts or suspicious activity, never engaging in transactions/interacting with businesses she doesn't trust and/or non-reputable vendors, using free identity theft/credit monitoring services and routinely checking same, regularly reviewing financial and other important account activity, storing important documents in a safe place, never transmitting her Social Security number to unknown/untrusted individuals/entities, and shredding/destroying sensitive documents.

56. Plaintiff Cruciata anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Cruciata will continue to be at present and continued increased risk of identity theft and fraud for years to come.

57. Plaintiff Cruciata has a continuing interest in ensuring that her PHI and PII, which remains in Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

58. As a result of the Data Breach, Plaintiff Cruciata has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen PHI and PII, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft, time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct, time and expenses spent monitoring bank accounts for fraudulent activity, loss in value of her personal data, lost property in the form of her compromised PHI and PII, and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff Cruciata now faces a substantial risk that unauthorized third parties will further misuse her PHI and PII because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Personal Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of Personal Information CL0P exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Cruciata has

(1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen PHI and PII such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her PHI and PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time that she spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

59. Plaintiff Cruciata experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Cruciata would compensate her for the foregoing redressable injuries. Further, Plaintiff Cruciata seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of her PHI and PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

3. Plaintiff Benjamin Dieck

60. Plaintiff Benjamin Dieck ("Plaintiff Dieck") is, and was at all relevant times, an individual and citizen of Fayetteville, North Carolina.

61. Plaintiff Dieck has no known relationship with Colorado Department of Human Services or Maximus Human Services, Inc.

62. Plaintiff Dieck received a letter from Maximus Human Services, Inc. dated August 24, 2023, that informed him of "an incident that may involve some of your personal information. Maximus is a contractor to the State of Colorado Department of Human Services, Division of Child Support Services (the Department) and provides services to support certain government programs including the State Directory of New Hires. Your information may have been involved

because the Department uses Maximus services to collect information employers are legally mandated to report to the Department and other Child Support Service divisions throughout the country. The incident involved a critical vulnerability in 'MOVEit Transfer,' a third-party software application provided by Progress Software Corporation (Progress)."

63. The letter states further as follows:

> **What Happened?**
> On May 30, 2023, Maximus detected unusual activity in our MOVEit environment. We promptly began to investigate and took the MOVEit environment offline early on May 31, 2023. The investigation determined that from approximately May 27 to May 31, 2023, an unauthorized party obtained copies of certain computer files saved in our MOVEit environment. We promptly notified the Department of the incident. Following further review of these files, we determined that those files contained some of your personal information.
>
> **What Information Was Involved?**
> The information involved may include your: name, social security number, address, and date of birth.

64. At the time that Progress discovered the data breach—on or around May 31, 2023—Defendants Progress and Maximus Human Services, Inc. retained Plaintiff Dieck's PII in their computer systems.

65. Accordingly, the letter states that Progress and Maximus Human Services, Inc. possessed Plaintiff Dieck's PII, including his name, Social Security number, address, and date of birth, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

66. According to the letter, Progress and Maximus Human Services, Inc. learned of the Data Breach as early as May 30-31, but they waited approximately three months before only Maximus Human Services, Inc. notified Plaintiff Dieck that his highly sensitive PII was compromised in the Data Breach.

67. In addition to their substantial delay in notifying Plaintiff Dieck of the Data Breach, Defendants also put the burden on Plaintiff Dieck to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

68. According to the letter, Defendants waited nearly three months before they notified Plaintiff Dieck that his Personal Information was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Dieck, who retains a vested interest in ensuring that his PII remains protected.

69. Moreover, Defendants' disclosure amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Dieck of the Data Breach's critical facts. Without those details, Plaintiff Dieck's ability to mitigate harms resulting from the Data Breach is severely diminished.

70. At the direction of Maximus Human Services, Inc., Plaintiff Dieck made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach and monitoring his accounts for suspicious activity. Plaintiff Dieck has spent significant time dealing with the Data Breach—valuable time Plaintiff Dieck otherwise would have put to profitable use, including, but not limited to, work and/or recreation. All told, Plaintiff Dieck estimates that he has spent approximately 45 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

71. The Data Breach has caused Plaintiff Dieck anxiety, sleep disruption, stress, anger, fear for his personal financial security, and fear for what information was revealed in the Data

Breach, which has been compounded by Defendants' nearly 3-month delay in informing him of the fact that his PII, including his Social Security number, was acquired by known cybercriminals through the Data Breach.

72. Plaintiff Dieck has also experienced a large uptick in fraudulent spam and phishing calls and emails since the Data Breach. Plaintiff Dieck is a government employee and as such receives quarterly training on identity protection; nevertheless, as a result of the Data Breach, he has increased the amount of time that he spends on monitoring his accounts to protect himself from identity theft and fraud.

73. Plaintiff Dieck greatly values his privacy and PII and takes reasonable steps to maintain the confidentiality of his PII, including maintaining strong passwords; regularly changing passwords; using multi-factor authentication; promptly investigating any alerts about login attempts or suspicious activity; refusing to engage in transactions/interacting with businesses he doesn't trust and/or non-reputable vendors; using free identity theft/credit monitoring services and routinely checking same; regularly reviewing financial and other important account activity; storing important documents in a safe place; never transmitting his Social Security number to unknown/ untrusted individuals/entities; and shredding/destroying sensitive documents.

74. Plaintiff Dieck anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Dieck will continue to be at present and continued increased risk of identity theft and fraud for years to come.

75. Plaintiff Dieck has a continuing interest in ensuring that his PII, which remains in Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

76. As a result of the Data Breach, Plaintiff Dieck has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of his stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft, time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct, time and expenses spent monitoring bank accounts for fraudulent activity, loss in value of his personal data, lost property in the form of his compromised PII, and injury to his privacy. Additionally, as a direct result of the Data Breach, Plaintiff Dieck now faces a substantial risk that unauthorized third parties will further misuse his PII because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Personal Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of Personal Information CL0P exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Dieck has (1) suffered, or is at an increased risk of suffering, unauthorized use of his stolen PII such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm because he lost time that he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort he expended addressing future consequences of the Data Breach.

77. Plaintiff Dieck experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Dieck would compensate him for the foregoing redressable injuries. Further, Plaintiff Dieck seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of his PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

4. Plaintiff Victor Diluigi

78. Plaintiff Victor Diluigi ("Plaintiff Diluigi") is, and was at all relevant times, an individual and citizen of York, Pennsylvania.

79. Plaintiff Victor Diluigi has no known relationship with the Arkansas Division of Workforce Services or Maximus Human Services, Inc.

80. Plaintiff Diluigi received a letter from Maximus Human Services, Inc. dated September 29, 2023, that informed him of "a data security incident that involved some of your personal information. Maximus is a contractor to the Arkansas Division of Workforce Services, (the "Agency") and provides services to support certain government programs. Your information was affected because this incident affected information shared with us by the Agency for administrative purposes. The incident involved a critical vulnerability in MOVEit Transfer, a third-party software application provided by Progress Software Corporation (Progress)."

81. The letter states further as follows:

> **What Happened?**
>
> On May 30, 2023, Maximus detected unusual activity in our MOVEit environment; we promptly began to investigate with the help of nationally recognized cybersecurity experts. Early in the day on May 31, 2023 we took our MOVEit application offline. Later that same day, Progress first publicly announced a

> previously unknown vulnerability in its MOVEIt software, which an unauthorized party used to gain access to files of many MOVEit customers. ***
>
> Maximus promptly notified the Agency of the Incident on June 2, 2023, and we have been working with them since. Additionally, we engaged a forensic investigation firm and a data analysis firm to identify affected individuals and the types of information involved. We learned that on approximately May 27-31, 2023, the unauthorized party obtained copies of certain files that were saved in the Maximus MOVEit application. After learning about the files, we began to analyze the files to determine which data was affected. After completing our investigation of the files related to the services Maximus provides to the Agency on September 8, 2023, we determined that those files contained some of your personal information.
>
> **What information was involved?**
> The information involved varied by individual and may include: name, Social Security number, date of birth, and address.

82. At the time that Progress discovered the data breach—on or around May 31, 2023—Defendants Progress and Maximus Human Services, Inc. retained Plaintiff Diluigi's PII in their computer systems.

83. Accordingly, the letter states that Progress and Maximus Human Services, Inc. possessed Plaintiff Diluigi's PII, including his name, Social Security number, address, and date of birth, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

84. According to the letter, Progress and Maximus Human Services, Inc. learned of the Data Breach as early as May 30-31, but they waited nearly four months before only Maximus Human Services, Inc. notified Plaintiff Diluigi that his highly sensitive PII was compromised in the Data Breach.

85. In addition to their substantial delay in notifying Plaintiff Diluigi of the Data Breach, Defendants also put the burden on Plaintiff Diluigi to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant by reviewing your financial

statements and accounts for signs of suspicious transactions and activities. Report any indications of suspected fraud or identify theft to local law enforcement, your State's Attorney General's office, or the Federal Trade Commission."

86. According to the letter, Defendants waited nearly four months before they notified Plaintiff Diluigi that his Personal Information was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Diluigi, who retains a vested interest in ensuring that his PII remains protected.

87. Moreover, Defendants' disclosure amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Diluigi of the Data Breach's critical facts. Without those details, Plaintiff Diluigi's ability to mitigate harms resulting from the Data Breach is severely diminished.

88. Plaintiff Diluigi's PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. More specifically, Plaintiff Diluigi has experienced multiple unauthorized charges on his credit cards and his debit card. On October 11, 2023, fraudulent charges were put on his Business Credit card in the amount of $99. While those charges were reimbursed, Plaintiff Diluigi, who is a long-distance truck driver, had to drive home from Georgia to get the new, replacement credit card. Plaintiff Diluigi later noticed a fraudulent $102.99 charge dated October 26, 2023 on his Business Debit card. That charge was temporarily credited and permanently repaid in November 2023. On February 25, 2024, Plaintiff Diluigi was fraudulently charged $43.38 on his personal credit card. Fraud prevention caught this and he did not get charged, but his card was shut down and he had to come home from Georgia to replace the card.

89. Further, at the direction of Maximus Human Services, Inc., Plaintiff Diluigi made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, contacting Maximus and/or Arkansas Division of Workforce Services about the Data Breach, contacting card issuers/banks to preemptively get new numbers, major credit bureaus to freeze his credit, monitoring accounts for suspicious activity, investigating suspicious activity, and contacting banks, credit card companies, and/or other businesses about suspicious activity–valuable time Plaintiff Diluigi otherwise would have put to profitable use, including, but not limited to, work and/or recreation. All told, Plaintiff Diluigi estimates that he has spent approximately 45 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

90. The Data Breach has caused Plaintiff Diluigi anxiety, sleep disruption, stress, anger, fear for his personal financial security, and fear for what information was revealed in the Data Breach, which has been compounded by Defendants' nearly 4-month delay in informing him of the fact that his PII, including his Social Security number, was acquired by known cybercriminals through the Data Breach.

91. Plaintiff Diluigi has also experienced a large uptick in fraudulent spam and phishing calls and emails since the Data Breach.

92. Plaintiff Diluigi greatly values his privacy and PII and takes reasonable steps to maintain the confidentiality of his PII, including maintaining strong passwords; regularly changing passwords; using multi-factor authentication; promptly investigating any alerts about login attempts or suspicious activity; refusing to engage in transactions/interacting with businesses he doesn't trust and/or non-reputable vendors; using identity theft/credit monitoring services and routinely checking same; regularly reviewing financial and other important account activity;

storing important documents in a safe place; never transmitting his Social Security number to unknown/ untrusted individuals/entities; and shredding/destroying sensitive documents.

93. Plaintiff Diluigi anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Diluigi will continue to be at present and continued increased risk of identity theft and fraud for years to come.

94. Plaintiff Diluigi has a continuing interest in ensuring that his PII, which remains in Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

95. As a result of the Data Breach, Plaintiff Diluigi has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of his stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft, time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct, time and expenses spent monitoring bank accounts for fraudulent activity, loss in value of his personal data, lost property in the form of his compromised PII, and injury to his privacy. Additionally, as a direct result of the Data Breach, Plaintiff Diluigi now faces a substantial risk that unauthorized third parties will further misuse his PII because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Personal Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of Personal Information CL0P exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data

Breach, Plaintiff Diluigi has (1) suffered, or is at an increased risk of suffering, unauthorized use of his stolen PII such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm because he lost time that he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort he expended addressing future consequences of the Data Breach.

96. Plaintiff Diluigi experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Diluigi would compensate him for the foregoing redressable injuries. Further, Plaintiff Diluigi seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of his PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

5. Plaintiffs S.K. and M.K.

97. Plaintiffs S.K. and M.K., minors, are and at all relevant times were, individuals and residents of Sanford, Florida. S.K. and M.K. bring this suit by and through their father and legal guardian, Aunali Khaku, who is, and was at all relevant times, an individual and citizen of Sanford, Florida.

98. Plaintiffs S.K. and M.K. have received medical services through the Florida Healthy Kids Corporation. In order to have their medical claims processed, Plaintiffs S.K. and M.K.'s father and legal guardian, Aunali Khaku, was required to provide his children's PII to Maximus, Inc.

99. Plaintiffs S.K. and M.K. received identical letters from Maximus, Inc. dated August 11, 2023, that informed them of "an incident that may have involved your personal health information. Maximus provides administrative services to the Florida Healthy Kids Corporation (Healthy Kids) to support its health insurance program. Maximus uses a software called MOVEit Transfer, a third-party software application provided Progress Software Corporation (Progress). The incident involved a critical vulnerability in MOVEit Transfer."

100. The letter states further as follows:

> **What happened?**
> On May 30, 2023, Maximus detected unusual activity in our MOVEit environment. We promptly began to investigate with the help of nationally recognized cybersecurity experts. On May 31, 2023, Maximus took our MOVEit application offline. Later that same day, Progress first publicly announced a problem with its MOVEit software, which allowed an unauthorized person to gain access to files of many MOVEit customers, including Maximus.
>
> Maximus promptly informed Healthy Kids of the incident and we have been working with them since. Additionally, we engaged a forensic investigation firm and a data analysis firm to identify affected individuals and the types of information involved. We learned that on approximately May 27 - May 31, 2023, the unauthorized person obtained copies of certain files that were saved in the Maximus MOVEit application. We then began to analyze the files to determine which data was affected and on June 12, 2023, determined filed related to Healthy Kids were impacted. Our investigation determined that the files contained some of your family's personal information.
>
> **What information Was involved?**
> Although the information impacted by the incident varied by individual, the information involved may include:
>
> - Name, address, date of birth, phone number, email address
> - Social Security number, other government-issued identifier
> - Tribal identification or enrollment number
> - Family Account Number

101. At the time that Progress discovered the data breach—on or around May 31, 2023—Defendants Progress and Maximus, Inc. retained Plaintiffs S.K. and M.K's PII in their computer systems.

102. Accordingly, the letter states that Progress and Maximus, Inc. possessed Plaintiffs S.K. and M.K.'s PII, including their name, address, date of birth, phone number, email address, Social Security number, other government-issued identifier, Tribal identification or enrollment number, and Family Account Number, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

103. According to the letter, Progress and Maximus, Inc. learned of the Data Breach as early as May 30-31, but they waited over two months before only Maximus, Inc. notified Plaintiffs S.K. and M.K. that their highly sensitive PII was compromised in the Data Breach.

104. In addition to their substantial delay in notifying Plaintiffs S.K. and M.K. of the Data Breach, Defendants also put the burden on Plaintiffs S.K. and M.K. to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant by reviewing your financial statements and accounts for signs of suspicious transactions and activities. Report any indications of suspected fraud or identify theft to local law enforcement, your State's Attorney General's office, or the Federal Trade Commission."

105. According to the letter, Defendants waited over two months before they notified Plaintiffs S.K. and M.K. that their Personal Information was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiffs S.K. and M.K., who retain a vested interest in ensuring that their PII remains protected.

106. Moreover, Defendants' disclosure amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiffs S.K. and M.K. of the Data Breach's critical facts.

Without those details, Plaintiffs S.K. and M.K.'s ability to mitigate harms resulting from the Data Breach is severely diminished.

107. At the direction of Maximus, Inc., Plaintiffs S.K. and M.K., through their father Aunali Khaku, made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, monitoring accounts for suspicious activity, investigating suspicious activity, and contacting banks, credit card companies, and/or other businesses about suspicious activity. Plaintiffs S.K. and M.K., through their father Aunali Khaku, have spent significant time dealing with the Data Breach—valuable time that would otherwise have been put to profitable use, including, but not limited to, work and/or recreation. All told, Plaintiffs S.K. and M.K., through their father Aunali Khaku, have spent approximately 40 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

108. The Data Breach has caused Plaintiffs S.K. and M.K., through their father Aunali Khaku, fear, anxiety, sleep disruption, stress, anger, fear for their personal financial security, and fear for what information was revealed in the Data Breach, which has been compounded by Defendants' over 2-month delay in informing them of the fact that their PII, including their Social Security numbers, were acquired by known cybercriminals through the Data Breach.

109. Plaintiffs S.K. and M.K. have also experienced a large uptick in fraudulent spam and phishing calls and emails in their names since the Data Breach.

110. Plaintiffs S.K. and M.K., through their father Aunali Khaku, take reasonable steps to maintain the confidentiality of PII, including maintaining strong passwords, regularly changing passwords, using multi-factor authentication, promptly investigating any alerts about login attempts or suspicious activity, regularly reviewing financial and other important account activity,

storing important documents in a safe place, never transmitting social security numbers to unknown/untrusted individuals/entities, and shredding/destroying sensitive documents

111. Plaintiffs S.K. and M.K., through their father Aunali Khaku, anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiffs S.K. and M.K. will continue to be at present and continued increased risk of identity theft and fraud for years to come.

112. Plaintiffs S.K. and M.K. have a continuing interest in ensuring that their PII, which remains in Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

113. As a result of the Data Breach, Plaintiffs S.K. and M.K. have already suffered—and are at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of their stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring their credit and for identity theft, time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct, time and expenses spent monitoring bank accounts for fraudulent activity, loss in value of their personal data, lost property in the form of their compromised PII, and injury to their privacy. Additionally, as a direct result of the Data Breach, Plaintiffs S.K. and M.K. now face a substantial risk that unauthorized third parties will further misuse their PII because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Personal Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of Personal Information CL0P exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as

fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiffs' names. As a result of the Data Breach, Plaintiffs S.K. and M.K. have (1) suffered, or are at an increased risk of suffering, unauthorized use of their stolen PII such that they have suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of their PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by their exposure to the risk of future harm because they lost time that they spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort expended addressing future consequences of the Data Breach.

114. Plaintiffs S.K. and M.K. experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiffs S.K. and M.K. would compensate them for the foregoing redressable injuries. Further, Plaintiffs S.K. and M.K. seek injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of their PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

6. Plaintiff Shellie Harper McCaskell

115. Plaintiff Shellie Harper McCaskell ("Plaintiff McCaskell") is, and was at all relevant times, an individual and citizen of Hemet, California.

116. Plaintiff McCaskell has received healthcare services from Medicare through the Centers for Medicare & Medicaid Services.

117. Plaintiff McCaskell received a letter from Maximus Federal Services, Inc. and the Centers for Medicare & Medicaid Services (CMS) dated July 28, 2023, that informed her of "an incident involving your personal information related to services provided by Maximus. The

incident involved a security vulnerability in the MOVEit software, a third-party application which allows for the transfer of files during the Medicare appeals process."

118. The letter states further as follows:

> **What Happened?** On May 30, 2023, Maximus detected unusual activity in its MOVEit application. Maximus began to investigate and stopped all use of the MOVEit application early on May 31, 2023. Later that same day, the third-party application provider, Progress Software Corporation, announced that a vulnerability in its MOVEit software had allowed an unauthorized party to gain access to files across many organizations in both the government and private sectors. Maximus notified CMS of the incident on June 2, 2023. To date, the ongoing investigation indicates that on approximately May 27 through May 31, 2023, the unauthorized party obtained copies of files that were saved in the Maximus MOVEit application, but that no CMS system has been compromised. As part of that analysis, it was determined that those files contained some of your personal information.
>
> **What Information Was Involved?** We have determined that your personal and Medicare information was involved in this incident. This information may have included the following:
>
> - Name
> - Social Security Numbers or Individual Taxpayer Identification Number
> - Date of Birth
> - Mailing Address
> - Telephone Number, Fax number, and Email Address
> - Medicare Beneficiary Identifier (MBI) or Health Insurance Claim Number (HICN)
> - Driver's License Number and State Identification Number
> - Medical history/ Notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.)
> - Healthcare Provider and Prescription Information
> - Health Insurance Claims and Policy/Subscriber Information
> - Health Benefits & Enrollment Information.

119. At the time that Progress discovered the data breach—on or around May 31, 2023—Defendants Progress and Maximus Federal Services, Inc. retained Plaintiff McCaskell's PHI and PII in their computer systems.

120. Accordingly, the letter states that Progress and Maximus Federal Services, Inc. possessed Plaintiff McCaskell's PHI and PII, including her Name, Social Security Numbers or

Individual Taxpayer Identification Number, Date of Birth, Mailing Address, Telephone Number, Fax number, and Email Address, Medicare Beneficiary Identifier (MBI) or Health Insurance Claim Number (HICN), Driver's License Number and State Identification Number, Medical history/ Notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.), Healthcare Provider and Prescription Information, Health Insurance Claims and Policy/Subscriber Information, and Health Benefits & Enrollment Information, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

121. According to the letter, Progress and Maximus Federal Services, Inc. learned of the Data Breach as early as May 30-31, but they waited approximately two months before only Maximus Federal Services, Inc. notified Plaintiff McCaskell that her highly sensitive PHI and PII was compromised in the Data Breach.

122. In addition to their substantial delay in notifying Plaintiff McCaskell of the Data Breach, Defendants also put the burden on Plaintiff McCaskell to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant by reviewing your financial statements and accounts for signs of suspicious transactions and activities. Report any indications of suspected fraud or identify theft to local law enforcement, your State's Attorney General's office, or the Federal Trade Commission."

123. According to the letter, Defendants waited two months before they notified Plaintiff McCaskell that her Personal Information was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff McCaskell, who retains a vested interest in ensuring that her PHI and PII remains protected.

124. Moreover, Defendants' disclosure amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff McCaskell of the Data Breach's critical facts. Without those details, Plaintiff McCaskell's ability to mitigate harms resulting from the Data Breach is severely diminished.

125. Plaintiff McCaskell experienced out of pocket postage costs as a result of the Data Breach when in response to the July 28, 2023 letter from Maximus Federal Services, Inc., Plaintiff McCaskell mailed in a request for her credit report. Further, at the direction of Maximus Federal Services, Inc., Plaintiff McCaskell made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, monitoring her accounts for suspicious activity, and reviewing her credit reports for suspicious activity. Plaintiff McCaskell has spent significant time dealing with the Data Breach—valuable time Plaintiff McCaskell otherwise would have put to profitable use, including, but not limited to, work and/or recreation. All told, Plaintiff McCaskell estimates that she has spent approximately 8 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

126. The Data Breach has caused Plaintiff McCaskell fear, anxiety, stress, sleep disruption, fear for her personal financial security, and fear for what information was revealed in the Data Breach, which has been compounded by Defendants' 2-month delay in informing her of the fact that her PHI and PII, including her Social Security number, was acquired by known cybercriminals through the Data Breach.

127. Plaintiff McCaskell has also experienced a large uptick in fraudulent spam and phishing calls and emails since the Data Breach, including near daily phone calls requesting that she purchase medical devices in late 2023.

128. Plaintiff McCaskell greatly values her privacy and PHI and PII and takes reasonable steps to maintain the confidentiality of her PHI and PII, including maintaining strong passwords, promptly investigating any alerts about login attempts or suspicious activity, never engaging in transactions/interacting with businesses she doesn't trust and/or non-reputable vendors, using free identity theft/credit monitoring services and routinely checking same, regularly reviewing financial and other important account activity, storing important documents in a safe place, never transmitting her Social Security number to unknown/untrusted individuals/entities, and shredding/destroying sensitive documents.

129. Plaintiff McCaskell anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff McCaskell will continue to be at present and continued increased risk of identity theft and fraud for years to come.

130. Plaintiff McCaskell has a continuing interest in ensuring that her PHI and PII, which remains in Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

131. As a result of the Data Breach, Plaintiff McCaskell has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen PHI and PII, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft, time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct, time and expenses spent monitoring bank accounts for fraudulent activity, loss in value of her personal data, lost property in the form of her compromised PHI and PII, and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff McCaskell now

faces a substantial risk that unauthorized third parties will further misuse her PHI and PII because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Personal Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of Personal Information CL0P exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff McCaskell has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen PHI and PII such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her PHI and PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time that she spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

132. Plaintiff McCaskell experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff McCaskell would compensate her for the foregoing redressable injuries. Further, Plaintiff McCaskell seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of her PHI and PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

7. Plaintiff Elaine McCoy

133. Plaintiff Elaine McCoy ("Plaintiff McCoy") is, and was at all relevant times, an individual and citizen of Tiffin, Ohio.

134. Plaintiff McCoy has received healthcare services from Medicare through the Centers for Medicare & Medicaid Services.

135. Plaintiff McCoy received a letter from Maximus Federal Services, Inc. and the Centers for Medicare & Medicaid Services (CMS) dated July 28, 2023, that informed her of "an incident involving your personal information related to services provided by Maximus. The incident involved a security vulnerability in the MOVEit software, a third-party application which allows for the transfer of files during the Medicare appeals process."

136. The letter states further as follows:

> **What Happened?** On May 30, 2023, Maximus detected unusual activity in its MOVEit application. Maximus began to investigate and stopped all use of the MOVEit application early on May 31, 2023. Later that same day, the third-party application provider, Progress Software Corporation, announced that a vulnerability in its MOVEit software had allowed an unauthorized party to gain access to files across many organizations in both the government and private sectors. Maximus notified CMS of the incident on June 2, 2023. To date, the ongoing investigation indicates that on approximately May 27 through May 31, 2023, the unauthorized party obtained copies of files that were saved in the Maximus MOVEit application, but that no CMS system has been compromised. As part of that analysis, it was determined that those files contained some of your personal information.
>
> **What Information Was Involved?** We have determined that your personal and Medicare information was involved in this incident. This information may have included the following:
>
> - Name
> - Social Security Numbers or Individual Taxpayer Identification Number
> - Date of Birth
> - Mailing Address
> - Telephone Number, Fax number, and Email Address
> - Medicare Beneficiary Identifier (MBI) or Health Insurance Claim Number (HICN)
> - Driver's License Number and State Identification Number

- Medical history/ Notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.)
- Healthcare Provider and Prescription Information
- Health Insurance Claims and Policy/Subscriber Information
- Health Benefits & Enrollment Information.

137. At the time that Progress discovered the data breach—on or around May 31, 2023—Defendants Progress and Maximus Federal Services, Inc. retained Plaintiff McCoy's PHI and PII in their computer systems.

138. Accordingly, the letter states that Progress and Maximus Federal Services, Inc. possessed Plaintiff McCoy's PHI and PII, including her Name, Social Security Numbers or Individual Taxpayer Identification Number, Date of Birth, Mailing Address, Telephone Number, Fax number, and Email Address, Medicare Beneficiary Identifier (MBI) or Health Insurance Claim Number (HICN), Driver's License Number and State Identification Number, Medical history/ Notes (including medical record/account numbers, conditions, diagnoses, dates of service, images, treatments, etc.), Healthcare Provider and Prescription Information, Health Insurance Claims and Policy/Subscriber Information, and Health Benefits & Enrollment Information, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

139. According to the letter, Progress and Maximus Federal Services, Inc. learned of the Data Breach as early as May 30-31, but they waited approximately two months before only Maximus Federal Services, Inc. notified Plaintiff McCoy that her highly sensitive PHI and PII was compromised in the Data Breach.

140. In addition to their substantial delay in notifying Plaintiff McCoy of the Data Breach, Defendants also put the burden on Plaintiff McCoy to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant by reviewing your financial statements and accounts for signs of suspicious transactions and activities. Report any indications

of suspected fraud or identify theft to local law enforcement, your State's Attorney General's office, or the Federal Trade Commission."

141. According to the letter, Defendants waited two months before they notified Plaintiff McCoy that her Personal Information was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff McCoy, who retains a vested interest in ensuring that her PHI and PII remains protected.

142. Moreover, Defendants' disclosure amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff McCoy of the Data Breach's critical facts. Without those details, Plaintiff McCoy's ability to mitigate harms resulting from the Data Breach is severely diminished.

143. Plaintiff McCoy's PHI and PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. More specifically, Plaintiff McCoy has experienced unauthorized charges on multiple credit cards, including an $89 charge on her Wayfair credit card on September 1, 2023, and a charge for around $200 in February 2024 on her Loft credit card. Plaintiff McCoy successfully disputed the charges and then cancelled both credit cards. Further, at the direction of Maximus Federal Services, Inc., Plaintiff McCoy made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, monitoring her accounts for suspicious activity, and contacting banks, credit card companies, and other businesses about suspicious activity. Plaintiff McCoy has spent significant time dealing with the Data Breach–valuable time Plaintiff McCoy otherwise would have put to profitable use, including, but not limited to, work and/or recreation.

All told, Plaintiff McCoy estimates that she has spent approximately 60 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

144. The Data Breach has caused Plaintiff McCoy fear, anxiety, stress, sleep disruption, anger, fear for her personal financial security, and fear for what information was revealed in the data breach, which has been compounded by Defendants' 2-month delay in informing her of the fact that her PHI and PII, including her Social Security number, was acquired by known cybercriminals through the Data Breach.

145. Plaintiff McCoy has also experienced a large uptick in fraudulent spam and phishing calls and emails since the Data Breach.

146. Plaintiff McCoy greatly values her privacy and PHI and PII and takes reasonable steps to maintain the confidentiality of her PHI and PII, including maintaining strong passwords, regularly changing passwords, using multi-factor authentication, promptly investigating any alerts about login attempts or suspicious activity, never engaging in transactions/interacting with businesses she doesn't trust and/or non-reputable vendors, using free identity theft/credit monitoring services and routinely checking same, regularly reviewing financial and other important account activity, storing important documents in a safe place, never transmitting her social security number to unknown/untrusted individuals/entities, and shredding/destroying sensitive documents

147. Plaintiff McCoy anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff McCoy will continue to be at present and continued increased risk of identity theft and fraud for years to come.

148. Plaintiff McCoy has a continuing interest in ensuring that her PHI and PII, which remains in Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

149. As a result of the Data Breach, Plaintiff McCoy has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen PHI and PII, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft, time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct, time and expenses spent monitoring bank accounts for fraudulent activity, loss in value of her personal data, lost property in the form of her compromised PHI and PII, and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff McCoy now faces a substantial risk that unauthorized third parties will further misuse her PHI and PII because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Personal Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of Personal Information CL0P exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff McCoy has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen PHI and PII such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her PHI and PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost

time that she spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

150. Plaintiff McCoy experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff McCoy would compensate her for the foregoing redressable injuries. Further, Plaintiff McCoy seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of her PHI and PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

8. Plaintiff Robert Plotke

151. Plaintiff Robert Plotke ("Plaintiff Plotke") is, and was at all relevant times, an individual and citizen of Plainfield, Illinois.

152. Plaintiff Plotke has been covered by certain Financial Institution Data Matching laws.

153. Plaintiff Plotke received a letter from Maximus, Inc. dated November 30, 2023, that informed him of "an incident involved certain of your information. Maximus is a contractor for the State of Minnesota. Your information was affected because this Incident affected information shared with us and by us for administrative purposes in accordance with Financial Institution Data Matching (FIDM) laws. FIDM data is submitted to Maximus by financial institutions that do business in Minnesota, in compliance with both federal and state laws. The incident involved a critical vulnerability in the MOVEit transfer, a third-party software application provided by Progress Software Corporation (Progress)."

154. The letter states further as follows:

> **What Happened?** On May 30, 2023, Maximus detected unusual activity in our MOVEit environment; we promptly began to investigate with the help of nationally recognized cybersecurity experts. Early in the day on May 31, 2023, Maximus took our MOVEit application offline. Later that same day, Progress first publicly announced a previously unknown vulnerability in its MOVEit software, which an unauthorized party used to gain access to files of many MOVEit customers. ***
>
> Maximus promptly informed the State of the Incident and we have been providing periodic updates to them since. Additionally, we engaged a forensic investigation firm and a data analysis firm to identify affected individuals and the types of information involved. We learned that on approximately May 27 - May 31, 2023, the unauthorized party obtained copies of certain files that were saved in the Maximus MOVEit application. After learning about the files, we began to analyze the files to determine which data was affected. We determined that the affected files contained some of your personal information.
>
> **What Information Was Involved?** The information involved may include your name, Social Security number, individual Taxpayer Identification number, address, date of birth and financial account number.

155. At the time that Progress discovered the data breach—on or around May 31, 2023—Defendants Progress and Maximus, Inc. retained Plaintiff Plotke's PII in their computer systems.

156. Accordingly, the letter states that Progress and Maximus, Inc. possessed Plaintiff Plotke's PII, including his name, Social Security number, individual Taxpayer Identification number, address, date of birth and financial account number, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

157. According to the letter, Progress and Maximus, Inc. learned of the Data Breach as early as May 30-31, but they waited approximately six months before only Maximus, Inc. notified Plaintiff Plotke that his highly sensitive PII was compromised in the Data Breach.

158. In addition to their substantial delay in notifying Plaintiff Plotke of the Data Breach, Defendants also put the burden on Plaintiff Plotke to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant by reviewing your financial statements and accounts for signs of suspicious transactions and activities. Report any indications of suspected

fraud or identify theft to local law enforcement, your State's Attorney General's office, or the Federal Trade Commission."

159. According to the letter, Defendants waited six months before they notified Plaintiff Plotke that his Personal Information was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Plotke, who retains a vested interest in ensuring that his PII remains protected.

160. Moreover, Defendants' disclosure amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Plotke of the Data Breach's critical facts. Without those details, Plaintiff Plotke's ability to mitigate harms resulting from the Data Breach is severely diminished.

161. Plaintiff Plotke's PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. More specifically, a credit card was opened in Plaintiff Plotke's name in February 2024 without his permission, and a bill was sent to his house. Plaintiff Plotke incurred out-of-pocket expenses as a result of the Data Breach for postage to successfully dispute the fraudulent credit card account, and in fact Plaintiff Plotke was informed by Credit One on March 5, 2024 that the account was fraudulent. Further, at the direction of Maximus, Inc., Plaintiff Plotke made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, monitoring his accounts for suspicious activity, investigating suspicious activity, and contacting banks, credit card companies, and other businesses about suspicious activity. Plaintiff Plotke has spent significant time dealing with the Data Breach—valuable time Plaintiff Plotke otherwise would have put to profitable use, including, but not limited to, work and/or recreation. All told, Plaintiff Plotke estimates that he has

spent approximately 70 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

162. The Data Breach has caused Plaintiff Plotke anxiety, sleep disruption, stress, anger, fear for his personal financial security, and fear for what information was revealed in the Data Breach, which has been compounded by Defendants' 6-month delay in informing him of the fact that his PII, including his Social Security number, was acquired by known cybercriminals through the Data Breach.

163. Plaintiff Plotke has also experienced a large uptick in fraudulent spam and phishing calls and emails since the Data Breach.

164. Plaintiff Plotke greatly values his privacy and PII and takes reasonable steps to maintain the confidentiality of his PII, including maintaining strong passwords, regularly changing passwords, using multi-factor authentication, promptly investigating any alerts about login attempts or suspicious activity, never engaging in transactions/interacting with businesses he doesn't trust and/or non-reputable vendors, regularly reviewing financial and other important account activity, storing important documents in a safe place, never transmitting his social security number to unknown/untrusted individuals/entities, and shredding/destroying sensitive documents

165. Plaintiff Plotke anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Plotke will continue to be at present and continued increased risk of identity theft and fraud for years to come.

166. Plaintiff Plotke has a continuing interest in ensuring that his PII, which remains in Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

167. As a result of the Data Breach, Plaintiff Plotke has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of his stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft, time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct, time and expenses spent monitoring bank accounts for fraudulent activity, loss in value of his personal data, lost property in the form of his compromised PII, and injury to his privacy. Additionally, as a direct result of the Data Breach, Plaintiff Plotke now faces a substantial risk that unauthorized third parties will further misuse his PII because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Personal Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of Personal Information CL0P exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Plotke has (1) suffered, or is at an increased risk of suffering, unauthorized use of his stolen PII such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm because he lost time that he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort he expended addressing future consequences of the Data Breach.

168. Plaintiff Plotke experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Plotke would compensate him for the foregoing redressable injuries. Further, Plaintiff Plotke seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of his PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

9. Plaintiff Jvanne Rhodes

169. Plaintiff Jvanne Rhodes ("Plaintiff Rhodes") is, and was at all relevant times, an individual and citizen of Dallas, Texas.

170. Plaintiff Rhodes' four children are enrolled with and received healthcare services from the Texas Health and Human Services Commission. In order for her children to obtain medical services, Plaintiff Rhodes was required to provide her PHI and PII to Maximus, directly or indirectly.

171. Plaintiff Rhodes received a letter from Maximus, Inc. dated August 31, 2023, that informed her of "an incident that involved some of your Information. Maximus is a contractor to the Texas Health and Human Services Commission (the "Agency") and provides services to support certain government programs. Your information was affected because this incident affected information shared with us and by us for administrative purposes. The incident involved a critical vulnerability in MOVEit Transfer, a third-party software application provided by Progress Software Corporation (Progress)."

172. The letter states further as follows:

> **What Happened?** On May 30, 2023, Maximus detected unusual activity in our MOVEit environment; we promptly began to investigate, engaged nationally recognized cybersecurity experts to assist us, and took our MOVEit application

> offline early on May 31, 2023. Later that same day, Progress first publicly announced a previously unknown vulnerability in its MOVEit software, which an unauthorized party used to gain access to certain within the MOVEit environments of many organizations. Maximus notified the Agency of the incident on June 9, 2023, and we have been working with them since the notification. The investigation determined that on approximately May 27 - May 31, 2023, the unauthorized party obtained copies of certain files that were saved in the Maximus MOVEit application. After making this determination, we began to analyze the files to determine which data had been affected. As part of that analysis, it was determined on June 12, 2023, that files for the Agency were impacted. Our investigation determined that the files contained some of your personal information.
>
> **What Information Was Involved?** Although the information impacted by this incident varied by individual, the information involved may include: Name, address, date of birth, Social Security Number, email, phone number, and dates of service.

173. At the time that Progress discovered the data breach—on or around May 31, 2023—Defendants Progress and Maximus, Inc. retained Plaintiff Rhodes's PHI and PII in their computer systems. Accordingly, the letter states that Progress and Maximus, Inc. possessed Plaintiff Rhodes's PHI and PII, including her name, address, date of birth, Social Security number, email, phone number, and dates of service, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

174. According to the letter, Progress and Maximus, Inc. learned of the Data Breach as early as May 30-31, but they waited approximately three months before only Maximus, Inc. notified Plaintiff Rhodes that her highly sensitive PHI and PII was compromised in the Data Breach.

175. In addition to their substantial delay in notifying Plaintiff Rhodes of the Data Breach, Defendants also put the burden on Plaintiff Rhodes to prevent any further harm resulting from the Data Breach by stating in the letter: "it is recommended that you regularly monitor account statements and monitor free credit reports. If you identify suspicious activity, you should contact the company that maintains the account on your behalf."

176. According to the letter, Defendants waited three months before they notified Plaintiff Rhodes that her Personal Information was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Rhodes, who retains a vested interest in ensuring that her PHI and PII remains protected.

177. Moreover, Defendants' disclosure amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Rhodes of the Data Breach's critical facts. Without those details, Plaintiff Rhodes's ability to mitigate harms resulting from the Data Breach is severely diminished.

178. Plaintiff Rhodes' PHI and PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. More specifically Plaintiff Rhodes incurred a fraudulent debit card charge on June 15, 2023, which caused her to cancel the card. Further, Plaintiff Rhodes has also been notified that an unknown person has tried to open accounts in her name without her authorization in July 2023. Further, at the direction of Maximus, Inc., Plaintiff Rhodes made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, monitoring her accounts for suspicious activity, and reviewing her credit reports for suspicious activity. Plaintiff Rhodes has spent significant time dealing with the Data Breach—valuable time Plaintiff Rhodes otherwise would have put to profitable use, including, but not limited to, work and/or recreation. All told, Plaintiff Rhodes estimates that she has spent approximately 175 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

179. The Data Breach has caused Plaintiff Rhodes anxiety, sleep disruption, stress, anger, very upset, physical pain (headaches/migraines, chest pains, upset stomach), fear for her

personal financial security, and fear for what information was revealed in the data breach, which has been compounded by Defendants' 3-month delay in informing her of the fact that her PHI and PII, including her Social Security number, was acquired by known cybercriminals through the Data Breach.

180. Plaintiff Rhodes has also experienced a large uptick in fraudulent spam and phishing calls and emails since the Data Breach.

181. Plaintiff Rhodes greatly values her privacy and PHI and PII and takes reasonable steps to maintain the confidentiality of her PHI and PII, including maintaining strong passwords, regularly changing passwords, using multi-factor authentication, promptly investigating any alerts about login attempts or suspicious activity, never engaging in transactions/interacting with businesses she doesn't trust and/or non-reputable vendors, using free identity theft/credit monitoring services; routinely checking same, regularly reviewing financial and other important account activity, storing important documents in a safe place, never transmitting her social security number to unknown/untrusted individuals/entities, and shredding/destroying sensitive documents.

182. Plaintiff Rhodes anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Rhodes will continue to be at present and continued increased risk of identity theft and fraud for years to come.

183. Plaintiff Rhodes has a continuing interest in ensuring that her PHI and PII, which remains in Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

184. As a result of the Data Breach, Plaintiff Rhodes has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the

unauthorized use of her stolen PHI and PII, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft, time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct, time and expenses spent monitoring bank accounts for fraudulent activity, loss in value of her personal data, lost property in the form of her compromised PHI and PII, and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff Rhodes now faces a substantial risk that unauthorized third parties will further misuse her PHI and PII because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Personal Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of Personal Information CL0P exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Rhodes has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen PHI and PII such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her PHI and PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time that she spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

185. Plaintiff Rhodes experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein

by Plaintiff Rhodes would compensate her for the foregoing redressable injuries. Further, Plaintiff Rhodes seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of her PHI and PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

10. Plaintiffs M.P. and M.Y.

186. Plaintiffs M.P. and M.Y., minors, are and at all relevant times were, individuals and residents of Allen, Texas. M.P. and M.Y. bring this suit by and through their mother and legal guardian, Aldreamer Smith, who is, and was at all relevant times, an individual and citizen of Allen, Texas.

187. Plaintiffs M.P. and M.Y. are enrolled with and received healthcare services from the Texas Health and Human Services Commission. In order to receive medical services, Plaintiffs M.P. and M.Y.'s mother and legal guardian, Aldreamer Smith, was required to provide her children's PHI and PII to Maximus, directly or indirectly.

188. Plaintiffs M.P. and M.Y.'s mother, Aldreamer Smith, received two identical letters addressed "To the Parent or Guardian of" M.P. and M.Y. from Maximus, Inc. dated September 9, 2023, that informed her of "an incident that involved some of your minor's Information. Maximus is a contractor to the Texas Health and Human Services Commission (the "Agency") and provides services to support certain government programs. Your minor's information was affected because this incident affected information shared with us and by us for administrative purposes. The incident involved a critical vulnerability in MOVEit Transfer, a third-party software application provided by Progress Software Corporation (Progress)."

189. The letters state further as follows:

> **What Happened?** On May 30, 2023, Maximus detected unusual activity in our MOVEit environment; we promptly began to investigate, engaged nationally recognized cybersecurity experts to assist us, and took our MOVEit application offline early on May 31, 2023. Later that same day, Progress first publicly announced a previously unknown vulnerability in its MOVEit software, which an unauthorized party used to gain access to certain within the MOVEit environments of many organizations. Maximus notified the Agency of the incident on June 9, 2023, and we have been working with them since the notification. The investigation determined that on approximately May 27 - May 31, 2023, the unauthorized party obtained copies of certain files that were saved in the Maximus MOVEit application. After making this determination, we began to analyze the files to determine which data had been affected. As part of that analysis, it was determined on June 12, 2023, that files for the Agency were impacted. Our investigation determined that the files contained some of your minor's personal information.
>
> **What Information Was Involved?** Although the information impacted by this incident varied by individual, the information involved may include: Name, address, date of birth, Social Security Number, email, phone number, and dates of service.

190. At the time that Progress discovered the data breach—on or around May 31, 2023—Defendants Progress and Maximus, Inc. retained Plaintiffs M.P. and M.Y.'s PHI and PII in their computer systems. Accordingly, the letter states that Progress and Maximus, Inc. possessed Plaintiffs M.P. and M.Y.'s PHI and PII, including their names, address, dates of birth, Social Security numbers, emails, phone numbers, and dates of service, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

191. According to the letter, Progress and Maximus, Inc. learned of the Data Breach as early as May 30-31, but they waited over three months before only Maximus, Inc. notified Plaintiffs M.P. and M.Y. that their highly sensitive PHI and PII was compromised in the Data Breach.

192. In addition to their substantial delay in notifying Plaintiffs M.P. and M.Y. of the Data Breach, Defendants also put the burden on Plaintiffs M.P. and M.Y., through their mother and legal guardian Aldreamer Smith, to prevent any further harm resulting from the Data Breach

by stating in the letters: "it is recommended that you regularly monitor account statements and monitor free credit reports. If you identify suspicious activity, you should contact the company that maintains the account on your behalf."

193. According to the letters, Defendants waited over three months before they notified Plaintiffs M.P. and M.Y. that their Personal Information was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiffs M.P. and M.Y., who retain a vested interest in ensuring that their PHI and PII remains protected.

194. Moreover, Defendants' disclosure amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiffs M.P. and M.Y. of the Data Breach's critical facts. Without those details, Plaintiffs M.P. and M.Y.'s ability to mitigate harms resulting from the Data Breach is severely diminished.

195. At the direction of Maximus, Inc., Plaintiffs M.P. and M.Y., through their mother and legal guardian Aldreamer Smith, made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, contacting credit bureaus, monitoring accounts for suspicious activity, investigating suspicious activity, and contacting banks, credit card companies, and/or other businesses about suspicious activity. Plaintiffs M.P. and M.Y. have spent significant time dealing with the Data Breach—valuable time Plaintiffs M.P. and M.Y. otherwise would have put to profitable use, including, but not limited to, work and/or recreation. All told, Plaintiffs M.P. and M.Y., through their mother and legal guardian Aldreamer Smith, estimate that approximately 8 hours has been

spent to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

196. The Data Breach has caused Plaintiffs M.P. and M.Y., through their mother and legal guardian Aldreamer Smith, fear, anxiety, stress, sleep disruption, fear for Plaintiffs' personal financial security, and fear for what information was revealed in the data breach, which has been compounded by Defendants' over 3-month delay in informing them of the fact that Plaintiffs' PHI and PII, including Social Security numbers, was acquired by known cybercriminals through the Data Breach.

197. Plaintiffs M.P. and M.Y. have also experienced a large uptick in fraudulent spam and phishing calls and emails since the Data Breach.

198. Plaintiffs M.P. and M.Y., through their mother and legal guardian Aldreamer Smith, greatly value their privacy and PHI and PII and take reasonable steps to maintain the confidentiality of their PHI and PII, including maintaining strong passwords, regularly changing passwords, using multi-factor authentication, promptly investigating any alerts about login attempts or suspicious activity, never engaging in transactions/interacting with businesses she doesn't trust and/or non-reputable vendors, using free identity theft/credit monitoring services and routinely checking same, regularly reviewing financial and other important account activity, storing important documents in a safe place, never transmitting social security numbers to unknown/untrusted individuals/entities, and shredding/destroying sensitive documents.

199. Plaintiffs M.P. and M.Y. through their mother and legal guardian Aldreamer Smith, anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiffs M.P. and M.Y. will continue to be at present and continued increased risk of identity theft and fraud for years to come.

200. Plaintiffs M.P. and M.Y. have a continuing interest in ensuring that their PHI and PII, which remains in Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

201. As a result of the Data Breach, Plaintiffs M.P. and M.Y. have already suffered—and are at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of their stolen PHI and PII, heightened threat of identity theft and general mitigation efforts spent on monitoring their credit and for identity theft, time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct, time and expenses spent monitoring bank accounts for fraudulent activity, loss in value of their personal data, lost property in the form of their compromised PHI and PII, and injury to their privacy. Additionally, as a direct result of the Data Breach, Plaintiffs M.P. and M.Y. now face a substantial risk that unauthorized third parties will further misuse their PHI and PII because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Personal Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of Personal Information CL0P exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiffs' names. As a result of the Data Breach, Plaintiffs M.P. and M.Y. have (1) suffered, or are at an increased risk of suffering, unauthorized use of their stolen PHI and PII such that they have suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of their PHI and PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by their exposure to the risk of future harm

because they lost time that they spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort they expended addressing future consequences of the Data Breach.

202. Plaintiffs M.P. and M.Y. experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiffs M.P. and M.Y. would compensate them for the foregoing redressable injuries. Further, Plaintiffs M.P. and M.Y. seek injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of their PHI and PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

11. Plaintiff Alexys Taylor

203. Plaintiff Alexys Taylor ("Plaintiff Taylor") was at all relevant times an individual and citizen of in Merrillville, Indiana, but is now a citizen of Michigan, residing in Grand Rapids, Michigan in September 2023.

204. Plaintiff Taylor has received Medicaid services through the Indiana Family and Social Services Administration.

205. Plaintiff Taylor received a letter from Maximus Health Services, Inc. dated August 11, 2023, that informed her of "an incident involving some of your information. Maximus is a contractor to the Indiana Family and Social Services Administration (the "Agency") and provides services to support certain government programs. Your information was affected because this incident involved information shared with us by the Agency for administrative purposes. *** This information involved may have included: Name, address, case number and recipient ID (RID). The RID is your Medicaid number. *** This incident involved a critical vulnerability in the

MOVEit software, a third-party software application provided by Progress Software Corporation (Progress)."

206. The letter states further as follows:

> **What Happened?** On May 30, 2023, Maximus detected unusual activity in our MOVEit environment; we promptly began to investigate, engaged nationally recognized cybersecurity experts to assist us, and took our MOVEit application offline early on May 31, 2023. Later that same day, Progress first publicly announced a previously unknown vulnerability in its MOVEit software, which an unauthorized party used to gain access to certain files within the MOVEit environments of many organizations.
>
> Maximus promptly informed the Agency of the incident, and we have been working with them since. Additionally, we engaged a forensic investigation firm and a data analysis firm to identify affected individuals and the types of information involved. We learned that on approximately May 27 - May 31, 2023, the unauthorized party obtained copies of certain files that were saved in the Maximus MOVEit application. After learning about the files, we began to analyze the files to determine which data was affected and on June 12, 2023 determined files related to the Agency were impacted. Our investigation determined that the files contained some of your personal information.

207. At the time that Progress discovered the data breach—on or around May 31, 2023—Defendants Progress and Maximus Health Services, Inc. retained Plaintiff Taylor's PHI and PII in their computer systems.

208. Accordingly, the letter states that Progress and Maximus Health Services, Inc. possessed Plaintiff Taylor's PHI and PII, including her Name, address, case number and Medicaid number, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

209. According to the letter, Progress and Maximus Health Services, Inc. learned of the Data Breach as early as May 30-31, but they waited over two months before only Maximus Health Services, Inc. notified Plaintiff Taylor that her highly sensitive PHI and PII was compromised in the Data Breach.

210. In addition to their substantial delay in notifying Plaintiff Taylor of the Data Breach, Defendants also put the burden on Plaintiff Taylor to prevent any further harm resulting from the Data Breach by stating in the letter: "it is recommended that you regularly monitor account statements and monitor free credit reports. If you identify suspicious activity, you should contact that company that maintains the account on your behalf."

211. According to the letter, Defendants waited two months before they notified Plaintiff Taylor that her Personal Information was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Taylor, who retains a vested interest in ensuring that her PHI and PII remains protected.

212. Moreover, Defendants' disclosure amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Taylor of the Data Breach's critical facts. Without those details, Plaintiff Taylor's ability to mitigate harms resulting from the Data Breach is severely diminished.

213. Plaintiff Taylor's PHI and PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. More specifically, shortly after the Data Breach, an unauthorized person used Plaintiff Taylor's RID to open both a gym membership at Planet Fitness and a Cash App account. Further, at the direction of Maximus Health Services, Inc., Plaintiff Taylor made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, monitoring her accounts for suspicious activity, and contacting banks, credit card companies, and other businesses about suspicious activity. Plaintiff Taylor has spent significant time dealing with the Data Breach—valuable time Plaintiff Taylor otherwise would have put to profitable use, including, but

not limited to, school work and/or recreation. All told, Plaintiff Taylor estimates that she has spent approximately 40 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

214. The Data Breach has caused Plaintiff Taylor anxiety, stress, fear for her personal financial security, and fear for what information was revealed in the data breach, which has been compounded by the fact that she received a notification that her Personal Information was on the dark web and by Defendants' 2-month delay in informing her of the fact that her PHI and PII was acquired by known cybercriminals through the Data Breach.

215. Plaintiff Taylor greatly values her privacy and PHI and PII and takes reasonable steps to maintain the confidentiality of her PHI and PII, including maintaining strong passwords, regularly changing passwords, using multi-factor authentication, promptly investigating any alerts about login attempts or suspicious activity, never engaging in transactions/interacting with businesses she doesn't trust and/or non-reputable vendors, using free identity theft/credit monitoring services and routinely checking same, regularly reviewing financial and other important account activity, storing important documents in a safe place, and never transmitting her Social Security number to unknown/untrusted individuals/entities.

216. Plaintiff Taylor anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Taylor will continue to be at present and continued increased risk of identity theft and fraud for years to come.

217. Plaintiff Taylor has a continuing interest in ensuring that her PHI and PII, which remains in Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

218. As a result of the Data Breach, Plaintiff Taylor has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen PHI and PII, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft, time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct, time and expenses spent monitoring bank accounts for fraudulent activity, loss in value of her personal data, lost property in the form of her compromised PHI and PII, and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff Taylor now faces a substantial risk that unauthorized third parties will further misuse her PHI and PII because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Personal Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of Personal Information CL0P exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Taylor has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen PHI and PII such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her PHI and PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time that she spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

219. Plaintiff Taylor experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Taylor would compensate her for the foregoing redressable injuries. Further, Plaintiff Taylor seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of her PHI and PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

B. Welltok Bellwether Plaintiffs

1. Plaintiff Tamara Williams

220. Plaintiff Tamara Williams ("Plaintiff Williams") is a resident and citizen of the state of Michigan and resides in Roseville, Michigan.

221. Plaintiff Williams is a current patient at Corewell Health, which, according to Plaintiff Williams's Notice Letter, contracted with Welltok to "operate[] a contact platform for Corewell Health East and received [Plaintiff Williams's] [Private Information] in connection with those services."

222. Plaintiff Williams received a Notice Letter by U.S. mail addressed to her directly from Welltok, writing on behalf of Corewell Health, dated November 17, 2023. According to the Notice Letter, Plaintiff Williams's Private Information was improperly accessed and obtained by unauthorized third parties, which may have included her "name, date of birth, email address, phone number, diagnosis, health insurance information, and Social Security Number."

223. Plaintiff Williams's Notice Letter states that:

> **What Happened.** On July 26, 2023, we were alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool. We had previously installed all published patches and security upgrades immediately upon such patches being made available by Progress Software, the maker of the MOVEit

> Transfer tool and conducted an examination of our systems and networks using all information available to determine the potential impact of the published vulnerabilities' presence on the MOVEit Transfer server and the security of data housed on the server and confirmed that there was no indication of any compromise at that time.
>
> Upon being alerted to the alleged issue, we moved quickly to launch an additional investigation with the assistance of third-party cybersecurity specialists and using additional information that had been discovered in the intervening period, to determine the potential for a hidden presence of vulnerabilities on the MOVEit Transfer server and the security of data housed on the server. After a full reconstruction of our systems and historical data, our investigation determined on August 11, 2023 that an unknown actor exploited software vulnerabilities, accessed the MOVEit Transfer server on May 30, 2023, and exfiltrated certain data from the MOVEit Transfer server during that time. We subsequently undertook a time-consuming and detailed reconstruction and review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data relates. Subsequently, we have learned that data related to you was present on the impacted server at the time of the event.

224. At the time that Progress discovered the Data Breach—on or around May 31, 2023—Welltok and Corewell Health were in possession and/or had stored Plaintiff Williams's Private Information but failed to protect it and, instead allowed cybercriminal to access it through the Data Breach. As Plaintiff Williams's Notice Letter acknowledges, after a "review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data relates[,]" Welltok "learned that data related to you was present on the impacted server at the time of the event."

225. Welltok and Corewell Health also failed to timely and adequately notify Plaintiff Williams about the Data Breach. Although the Notice Letter disclosed that Welltok had been "alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool," on July 26, 2023, it took Welltok and Corewell Health four months to notify Plaintiff Williams of the Data Breach's occurrence.

226. In addition to their substantial delay in notifying Plaintiff Williams of the Data Breach, Welltok and Corewell Health also put the burden on Plaintiff Williams to prevent any further harm resulting from the Data Breach by not disclosing the specific Private Information of Plaintiff Williams that was compromised or the specific actions taken by Welltok and Corewell Health in response to the Data Breach.

227. Instead, Plaintiff Williams's Notice Letter simply identified categories of Plaintiff Williams's Private Information that may or may not have been compromised by the Data Breach, stating that, "[t]he following types of information may have been impacted: name, date of birth, email address, phone number, diagnosis, health insurance information, and Social Security Number."

228. Plaintiff Williams's Notice Letter further stated vaguely that "we are reviewing and enhancing our existing policies and procedures related to data privacy to reduce the likelihood of a similar future event." The Notice Letter also advised Plaintiff Williams in general terms "to remain vigilant against incidents of identity theft and fraud by regularly reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

229. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Williams who retains a vested interest in ensuring that her Private Information remains protected.

230. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff Williams of the Data Breach's critical facts. Without these details, Plaintiffs Williams's ability to mitigate the harms resulting from the Data Breach is severely diminished.

231. Plaintiff Williams's Private Information compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. On or around November 2023, Plaintiff Williams was alerted by IdentityTheft.gov that someone had used her Social Security number to open a fraudulent account for internet services with a telecommunications company called Prosper Wireless, taking out a phone and a tablet. In addition, on or around March 2024, Plaintiff Williams was notified by a loan company called Lending Club that she was being denied a request for a $40,000 loan that an unauthorized person requested without her knowledge. Further, on or around June 2024, without Plaintiff Williams's knowledge, $9 had been withdrawn from a debit account that she had with Huntington Bank by an unauthorized person located in Ghana, which resulted in Huntington Bank closing that account. Further, on or around June 5, July 15, July 17, September 20, and September 30, Plaintiff Williams received threatening phishing calls and voicemail messages from unknown numbers showing up as spam on her phone, claiming that Plaintiff Williams has a fictitious back tax issue that she must fix by providing the caller with her social security number. Some of these calls have involved threats that Plaintiff Williams will be arrested if she does not verify her Social Security number and other personal information.

232. Since the Data Breach, Plaintiff Williams experienced other forms of spam and phishing emails, texts, and phone calls on a nearly daily basis, including texts claiming to be from the United States Postal Office, saying they are withholding deliveries from her until she clicks on a suspicious link to verify personal information. This misuse of her Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often

target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

233. Moreover, beginning on or around January 15, 2023, Plaintiff Williams has received notifications from Google Dark Web Report, reporting that Plaintiff Williams's private information had been found on the dark web.

234. As a result of the above fraudulent activity, Plaintiff Williams had to place a freeze on her credit with Experian, TransUnion, and Equifax, as well as change her email accounts and passwords numerous times.

235. As a direct and proximate result of the Data Breach, Plaintiff Williams has spent substantial time and effort on, among other things: investigating and taking remedial actions to the fraudulent/suspicious instances of fraud and identity theft identified above; contacting banks, credit card companies, and other vendors/companies (such as Prosper Wireless and Lending Club) regarding fraudulent/suspicious activity; investigating and checking the accuracy of the spam and phishing emails, texts, and phone calls she has received and continues to receive on a daily basis; placing freezes on her credit with Experian, TransUnion, and Equifax; changing passwords for sensitive accounts such as bank accounts; researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter; and monitoring her financial accounts for any indication of additional fraudulent activity on a daily basis.

236. Plaintiff Williams greatly values her privacy and her Private Information and takes reasonable steps to maintain the confidentiality of her Private Information including, among other things, maintaining strong passwords, regularly changing email and bank passwords, using multi-factor authentication for sensitive accounts, regularly reviewing financial and other important account activity, promptly investigating any alerts about login attempts or suspicious activity,

avoiding transactions with businesses she does not trust, using credit monitoring services, storing important documents in a safe place, and making sure that she has not shared her Social Security number publicly or directly to any unknown or untrusted individuals or entities.

237. Despite these efforts, Plaintiff Williams is very concerned about fraud and identity theft, as well as the consequences of such fraud and identity theft, resulting from the Data Breach. Specifically, the Data Breach has caused Plaintiff Williams to fear for her personal financial security "all the time" and feels "violated" over "someone else out there trying to become you" especially given the fraudulent activity and identity theft she has experienced. Plaintiff Williams was "distraught" from that activity. That the Data Breach has had an adverse effect on Plaintiff Williams is further apparent by the fact that she has actually cried from the daily harassing and threating spam and phishing texts and calls she receives daily and the physical pain she has experienced from some of the autoimmune conditions she has being exacerbated from the daily stress and anxiety caused by the Data Breach. Plaintiff Williams has also suffered a loss of sleep from staying awake through the night stressing over the Data Breach, including having stayed up until 5am every day for a full week investigating what happened with respect to the $40,000 loan that an unauthorized person tried to take out in her name. Plaintiff Williams stresses about having to worry about people constantly trying to rob and deceive her, and harass her to get income from her.

238. The daily stress, fear, and time spent by Plaintiff Williams as a result of the Data Breach has prevented and continues to prevent Plaintiff Williams from spending time on other things, such as "taking a meditation walk, or "trying a new recipe" or exercising at the local rec center." Instead, that time is spent waking up to harassing and threating messages on her phone from scammers that she must investigate and deal with. As Plaintiff Williams put it, these

consequences of the Data Breach "rob her of a level of enjoyment" of the day. This lost time can never be recovered.

239. Plaintiff Williams anticipates spending additional considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach, especially since she continues to be harassed with spam and phishing attempts to engage in fraud and identity theft at her expense on a daily basis. In addition, Plaintiff Williams will continue to be at present and continued increased risk of identity theft and fraud for years to come.

240. Plaintiff Williams has a continuing interest in ensuring that her Private Information, which remains in Progress's and Welltok Bellwether Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

241. As a result of the Data Breach, Plaintiff Williams has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen Private Information, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised Private Information; and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff Williams now faces a substantial risk that unauthorized third parties will further misuse her Private Information because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Private Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of Private Information CL0P exfiltrated in the Data Breach

is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff Williams's name. As a result of the Data Breach, Plaintiff Williams has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen Private Information such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her Private Information and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time that she spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

242. Plaintiff Williams experienced all of the foregoing harm and injury as a direct result of Progress and Welltok Bellwether Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Williams would compensate her for the foregoing redressable injuries. Further, Plaintiff Williams seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Progress and Welltok Bellwether Defendants to take steps to monitor for, protect, and/or prevent misuse of her Private Information accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

2. Plaintiff Jeffrey Weaver

243. Plaintiff Jeffrey Weaver ("Plaintiff Weaver") is a resident and citizen of the state of Michigan and resides in South Lyon, Michigan.

244. Plaintiff Weaver is a current patient at Corewell Health, which, according to Plaintiff Weaver's Notice Letter, contracted with Welltok to "operate[] a contact platform for

Corewell Health East and received [Plaintiff Weaver's] [Private Information] in connection with those services."

245. Plaintiff Weaver received a Notice Letter by U.S. mail addressed to him directly from Welltok, writing on behalf of Corewell Health, dated November 17, 2023. According to the Notice Letter, Plaintiff Weaver's Private Information was improperly accessed and obtained by unauthorized third parties, which may have included his "name, date of birth, email address, phone number, diagnosis, health insurance information, and Social Security Number."

246. Plaintiff Weaver's Notice Letter states that:

> **What Happened.** On July 26, 2023, we were alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool. We had previously installed all published patches and security upgrades immediately upon such patches being made available by Progress Software, the maker of the MOVEit Transfer tool and conducted an examination of our systems and networks using all information available to determine the potential impact of the published vulnerabilities' presence on the MOVEit Transfer server and the security of data housed on the server and confirmed that there was no indication of any compromise at that time.
>
> Upon being alerted to the alleged issue, we moved quickly to launch an additional investigation with the assistance of third-party cybersecurity specialists and using additional information that had been discovered in the intervening period, to determine the potential for a hidden presence of vulnerabilities' on the MOVEit Transfer server and the security of data housed on the server. After a full reconstruction of our systems and historical data, our investigation determined on August 11, 2023 that an unknown actor exploited software vulnerabilities, accessed the MOVEit Transfer server on May 30, 2023, and exfiltrated certain data from the MOVEit Transfer server during that time. We subsequently undertook a time-consuming and detailed reconstruction and review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data relates. Subsequently, we have learned that data related to you was present on the impacted server at the time of the event.

247. At the time that Progress discovered the Data Breach—on or around May 31, 2023—Welltok and Corewell Health were in possession or and/or had stored Plaintiff Weaver's Private Information but failed to protect it and, instead allowed cybercriminal to access it through the Data

Breach. As Plaintiff Weaver's Notice Letter acknowledges, after a "review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data relates[,]" Welltok "learned that data related to you was present on the impacted server at the time of the event."

248. Welltok and Corewell Health also failed to timely and adequately notify Plaintiff Weaver about the Data Breach. Although the Notice Letter disclosed that Welltok had been "alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool," on July 26, 2023, it took Welltok and Corewell Health *four months* to notify Plaintiff Weaver of the Data Breach's occurrence.

249. In addition to their substantial delay in notifying Plaintiff Weaver of the Data Breach, Welltok and Corewell Health also put the burden on Plaintiff Weaver to prevent any further harm resulting from the Data Breach by not disclosing the specific Private Information of Plaintiff Weaver that was compromised or the specific actions taken by Welltok and Corewell Health in response to the Data Breach.

250. Instead, Plaintiff Weaver's Notice Letter simply identified categories of Plaintiff Weaver's Private Information that may or may not have been compromised by the Data Breach, stating that, "[t]he following types of information may have been impacted: name, date of birth, email address, phone number, diagnosis, health insurance information, and Social Security Number."

251. Plaintiff Weaver's Notice Letter further stated vaguely that "we are reviewing and enhancing our existing policies and procedures related to data privacy to reduce the likelihood of a similar future event." The Notice Letter also advised Plaintiff Weaver in general terms "to remain

vigilant against incidents of identity theft and fraud by regularly reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

252. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Weaver who retains a vested interest in ensuring that his Private Information remains protected.

253. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff Weaver of the Data Breach's critical facts. Without these details, Plaintiff Weaver's ability to mitigate the harms resulting from the Data Breach is severely diminished.

254. Plaintiff Weaver's Private Information compromised in the Data Breach has already been circulated on the Dark Web. Indeed, Plaintiff Weaver has received numerous notifications from CapitalOne, Experian, and IDX Monitoring throughout 2024, as recently as October 16, 2024, stating that his Private Information, including his Social Security number specifically was found on the Dark Web.

255. Since the Data Breach, Plaintiff Weaver experienced other forms of spam and phishing emails, texts, and phone calls. This misuse of his Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

256. As a direct and proximate result of the Data Breach, Plaintiff Weaver has spent substantial time (approximately 200 hours since the Data Breach) and effort on, among other things: investigating and checking the accuracy of the spam and phishing emails, texts, and phone calls he has received and continues to receive; regularly changing passwords for sensitive accounts such as bank accounts; researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter; monitoring his financial accounts for any indication of fraudulent activity on a daily basis; and reviewing Dark Web notifications he receives.

257. Plaintiff Weaver greatly values his privacy and his Private Information and takes reasonable steps to maintain the confidentiality of his Private Information including, among other things, maintaining strong passwords, regularly changing his email and bank passwords, using multi-factor authentication whenever it is offered, regularly reviewing financial and other important account activity, promptly investigating any alerts about login attempts or suspicious activity, avoiding transactions with businesses he does not trust, using credit monitoring services, storing important documents in a safe place, using credit monitoring services, such as IDX, and making sure that he has not shared his Social Security number publicly or directly to any unknown or untrusted individuals or entities.

258. Despite these efforts, Plaintiff Weaver is very concerned about fraud and identity theft, as well as the consequences of such fraud and identity theft, resulting from the Data Breach. Specifically, the Data Breach has caused Plaintiff Weaver to experience stress, anxiety, and paranoia from knowing that his Social Security number has been found on the Dark Web, placing him at constant risk of experiencing fraudulent activity. Plaintiff Weaver has worked very hard to establish excellent credit and stresses over how that hard work could be undone by his credit being ruined as a result of his Social Security number being compromised. Plaintiff Weaver did not

experience his current level of stress and anxiety during his lifetime before the Data Breach took place. Further, Plaintiff Weaver has also suffered from sleep disruption as a result of the Data Breach and his Private Information being found on the Dark Web.

259. Plaintiff Weaver anticipates spending additional considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach, especially since he was informed that his Social Security number was found on the Dark Web. In addition, Plaintiff Weaver will continue to be at present and continued increased risk of identity theft and fraud for years to come.

260. Plaintiff Weaver has a continuing interest in ensuring that his Private Information, which remains in Progress and Welltok Bellwether Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

261. As a result of the Data Breach, Plaintiff Weaver has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of his stolen Private Information, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of his personal data; lost property in the form of his compromised Private Information; and injury to his privacy. Additionally, as a direct result of the Data Breach, Plaintiff Weaver now faces a substantial risk that unauthorized third parties will further misuse his Private Information because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Private Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized

conduct; and (3) the type of Private Information CL0P exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff Weaver's name. As a result of the Data Breach, Plaintiff Weaver has (1) suffered, or is at an increased risk of suffering, unauthorized use of his stolen Private Information such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his Private Information and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm because his lost time that he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort his expended addressing future consequences of the Data Breach.

262. Plaintiff Weaver experienced all of the foregoing harm and injury as a direct result of Progress and Welltok Bellwether Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Weaver would compensate him for the foregoing redressable injuries. Further, Plaintiff Weaver seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Progress and Welltok Bellwether Defendants to take steps to monitor for, protect, and/or prevent misuse of his Private Information accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

3. Plaintiff Amanda Copans

263. Plaintiff Amanda Copans ("Plaintiff Copans") is a resident and citizen of the state of California and resides in San Francisco, California.

264. Plaintiff Copans is a current patient at Sutter Health, which, according to Plaintiff Copans's Notice Letter, contracted with Welltok to "operate[] a contact platform for Sutter Health and received [Plaintiff Copans's] [Private Information] in connection with those services."

265. Plaintiff Copans received a Notice Letter by U.S. mail addressed to her directly from Welltok, writing on behalf of Sutter Health, dated October 31, 2023. According to the Notice Letter, Plaintiff Copans's Private Information was improperly accessed and obtained by unauthorized third parties, which may have included her "name, date of birth, health insurance information, provider name, treatment cost information, and treatment information or diagnosis."

266. Plaintiff Copans's Notice Letter states that:

> **What Happened.** On July 26, 2023, we were alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool. We had previously installed all published patches and security upgrades immediately upon such patches being made available by Progress Software, the maker of the MOVEit Transfer tool and conducted an examination of our systems and networks using all information available to determine the potential impact of the published vulnerabilities' presence on the MOVEit Transfer server and the security of data housed on the server and confirmed that there was no indication of any compromise at that time.
>
> Upon being alerted to the alleged issue, we moved quickly to launch an additional investigation with the assistance of third-party cybersecurity specialists and using additional information that had been discovered in the intervening period, to determine the potential for a hidden presence of vulnerabilities' on the MOVEit Transfer server and the security of data housed on the server. After a full reconstruction of our systems and historical data, our investigation determined on August 11, 2023 that an unknown actor exploited software vulnerabilities, accessed the MOVEit Transfer server on May 30, 2023, and exfiltrated certain data from the MOVEit Transfer server during that time. We subsequently undertook a time-consuming and detailed reconstruction and review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data relates. Subsequently, we have learned that data related to you was present on the impacted server at the time of the event.

267. At the time that Progress discovered the Data Breach—on or around May 31, 2023—Welltok and Sutter Health were in possession or had stored Plaintiff Copans's Private

Information but failed to protect it and, instead allowed cybercriminals to access it through the Data Breach. As Plaintiff Copans's Notice Letter acknowledges, after a "review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data relates[,]" Welltok "learned that data related to you was present on the impacted server at the time of the event."

268. Welltok and Sutter Health also failed to timely and adequately notify Plaintiff Copans about the Data Breach. Although the Notice Letter disclosed that Welltok had been "alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool," on July 26, 2023, it took Welltok and Sutter Health *over three months* to notify Plaintiff Copans of the Data Breach's occurrence.

269. In addition to their substantial delay in notifying Plaintiff Copans of the Data Breach, Welltok and Sutter Health also put the burden on Plaintiff Copans to prevent any further harm resulting from the Data Breach by not disclosing the specific Private Information of Plaintiff Copans that was compromised or the specific actions taken by Welltok and Sutter Health in response to the Data Breach.

270. Instead, Plaintiff Copans's Notice Letter simply identified categories of Plaintiff Copans's Private Information that may or may not have been compromised by the Data Breach, stating that, "[t]he following types of information may have been impacted: your name, and date of birth, health insurance information, provider name, treatment cost information, and treatment information or diagnosis."

271. Plaintiff Copans's Notice Letter further stated vaguely that "we are reviewing and enhancing our existing policies and procedures related to data privacy to reduce the likelihood of

a similar future event." The Notice Letter also advised Plaintiff Copans in general terms "to remain vigilant against incidents of identity theft and fraud by regularly reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

272. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Copans who retains a vested interest in ensuring that her Private Information remains protected.

273. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff Copans of the Data Breach's critical facts. Without these details, Plaintiffs Copans's ability to mitigate the harms resulting from the Data Breach is severely diminished.

274. Plaintiff Copans's Private Information compromised in the Data Breach has already been circulated on the Dark Web. Indeed, Plaintiff Copans has received numerous notifications from Norton this year, including one on August 23, 2024, stating that her Private Information, including her name and Social Security number specifically were found on the Dark Web. As a result of the Data Breach, Plaintiff Copans pays for annual credit monitoring services with Norton at an out-of-pocket cost of $8.99 per month.

275. Since the Data Breach, Plaintiff Copans experienced other forms of spam and phishing emails, texts, and phone calls. This misuse of her Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data

breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

276. As a direct and proximate result of the Data Breach, Plaintiff Copans has spent substantial time and effort on, among other things: investigating and checking the accuracy of the spam and phishing emails, texts, and phone calls she has received and continues to receive; regularly changing passwords for sensitive accounts such as bank accounts; researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter; monitoring her financial accounts and credit reports for any indication of fraudulent activity on a daily basis; and reviewing Dark Web notifications she receives.

277. Plaintiff Copans greatly values her privacy and her Private Information and takes reasonable steps to maintain the confidentiality of her Private Information including, among other things, maintaining strong passwords that she generates using Norton, regularly changing email and bank passwords, using multi-factor authentication for sensitive accounts, regularly reviewing financial and other important account activity, promptly investigating any alerts about login attempts or suspicious activity, avoiding transactions with businesses she does not trust, using credit monitoring services through Norton and Chase, storing important documents in a safe place, and making sure that she has not shared her Social Security number publicly or directly to any unknown or untrusted individuals or entities.

278. Despite these efforts, Plaintiff Copans is very concerned about fraud and identity theft, as well as the consequences of such fraud and identity theft, resulting from the Data Breach. Specifically, the Data Breach has caused Plaintiff Copans to experience stress and anxiety from her Social Security number being found on the Dark Web and not knowing what type of fraudulent activity or identity theft she could experience on any given day. Plaintiff Copans's concerns over

the Data Breach are compounded by the fact it involves private medical and health information, which she is particularly sensitive to given her occupation as a Vice President of Medical Affairs at a pharmaceutical company.

279. Plaintiff Copans anticipates spending additional considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Copans will continue to be at present and continued increased risk of identity theft and fraud for years to come.

280. Plaintiff Copans has a continuing interest in ensuring that her Private Information, which remains in Progress and Welltok Bellwether Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

281. As a result of the Data Breach, Plaintiff Copans has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen Private Information, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised Private Information; and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff Copans now faces a substantial risk that unauthorized third parties will further misuse her Private Information because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Private Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of Private Information CL0P exfiltrated in the Data Breach

is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff Copans's name. As a result of the Data Breach, Plaintiff Copans has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen Private Information such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her Private Information and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time that she spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

282. Plaintiff Copans experienced all of the foregoing harm and injury as a direct result of Progress and Welltok Bellwether Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Copans would compensate her for the foregoing redressable injuries. Further, Plaintiff Copans seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Progress and Welltok Bellwether Defendants to take steps to monitor for, protect, and/or prevent misuse of her Private Information accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

4. Plaintiff Denise Meyer

283. Plaintiff Denise Meyer ("Plaintiff Meyer") is a resident and citizen of the state of California and resides in Auburn, California.

284. Plaintiff Meyer is a current patient at Sutter Health, which, according to Plaintiff Meyer's Notice Letter, contracted with Welltok to "operate[] a contact platform for Sutter Health and received [Plaintiff Meyer's] [Private Information] in connection with those services."

285. Plaintiff Meyer received a Notice Letter by U.S. mail addressed to her directly from Welltok, writing on behalf of Sutter Health, dated October 31, 2023. According to the Notice Letter, Plaintiff Meyer's Private Information was improperly accessed and obtained by unauthorized third parties, which may have included her "name, date of birth, health insurance information, provider name, treatment cost information, and treatment information or diagnosis."

286. Plaintiff Meyer's Notice Letter states that:

> **What Happened.** On July 26, 2023, we were alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool. We had previously installed all published patches and security upgrades immediately upon such patches being made available by Progress Software, the maker of the MOVEit Transfer tool and conducted an examination of our systems and networks using all information available to determine the potential impact of the published vulnerabilities' presence on the MOVEit Transfer server and the security of data housed on the server and confirmed that there was no indication of any compromise at that time.
>
> Upon being alerted to the alleged issue, we moved quickly to launch an additional investigation with the assistance of third-party cybersecurity specialists and using additional information that had been discovered in the intervening period, to determine the potential for a hidden presence of vulnerabilities' on the MOVEit Transfer server and the security of data housed on the server. After a full reconstruction of our systems and historical data, our investigation determined on August 11, 2023 that an unknown actor exploited software vulnerabilities, accessed the MOVEit Transfer server on May 30, 2023, and exfiltrated certain data from the MOVEit Transfer server during that time. We subsequently undertook a time-consuming and detailed reconstruction and review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data relates. Subsequently, we have learned that data related to you was present on the impacted server at the time of the event.

287. At the time that Progress discovered the Data Breach—on or around May 31, 2023—Welltok and Sutter Health were in possession or and/or had stored Plaintiff Meyer's Private Information but failed to protect it and, instead allowed cybercriminal to access it through the Data Breach. As Plaintiff Meyer's Notice Letter acknowledges, after a "review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data

relates[,]" Welltok "learned that data related to you was present on the impacted server at the time of the event."

288. Welltok and Sutter Health also failed to timely and adequately notify Plaintiff Meyer about the Data Breach. Although the Notice Letter disclosed that Welltok had been "alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool," on July 26, 2023, it took Welltok and Sutter Health *over three months* to notify Plaintiff Meyer of the Data Breach's occurrence.

289. In addition to their substantial delay in notifying Plaintiff Meyer of the Data Breach, Welltok and Sutter Health also put the burden on Plaintiff Meyer to prevent any further harm resulting from the Data Breach by not disclosing the specific Private Information of Plaintiff Meyer that was compromised or the specific actions taken by Welltok and Sutter Health in response to the Data Breach.

290. Instead, Plaintiff Meyer's Notice Letter simply identified categories of Plaintiff Meyer's Private Information that may or may not have been compromised by the Data Breach, stating that, "[t]he following types of information may have been impacted: name, date of birth, health insurance information, provider name, treatment cost information, and treatment information or diagnosis."

291. Plaintiff Meyer's Notice Letter further stated vaguely that "we are reviewing and enhancing our existing policies and procedures related to data privacy to reduce the likelihood of a similar future event." The Notice Letter also advised Plaintiff Meyer in general terms "to remain vigilant against incidents of identity theft and fraud by regularly reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

292. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Meyer who retains a vested interest in ensuring that her Private Information remains protected.

293. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff Meyer of the Data Breach's critical facts. Without these details, Plaintiffs Meyer's ability to mitigate the harms resulting from the Data Breach is severely diminished.

294. Plaintiff Meyer's Private Information compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. For example, Plaintiff Meyer has received notification about two separate attempts made to access her Apple account; one on October 24, 2024 from Brazil and another earlier that same month from Sao Paula, saying that, "Apple ID Sign In Requested by [Plaintiff Meyer's email account]: Your Apple ID is being used to sign in to a Macbook Pro Near Sao Paulo." In addition, since the Data Breach, Plaintiff Meyer had unrecognized withdrawals from her debit account as a result of unauthorized purchases made, causing her to close that account. Plaintiff Meyer has also received telephone calls from an unknown individual who acquired her name, date of birth, and telephone number, claiming that her Private Information was found on the Dark Web and the only way for her to get it removed was to provide the caller with additional personal and financial information, which Plaintiff Meyer refused to provide. Further, Plaintiff Meyer had her GMAIL account hacked on or around August 2024, which resulted in her being locked out of the account.

295. Since the Data Breach, Plaintiff Meyer experienced other forms of spam and phishing emails, texts, and phone calls on a daily basis. This misuse of her Private Information

was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

296. As a direct and proximate result of the Data Breach, Plaintiff Meyer has spent substantial time (approximately 100+ hours and counting) and effort on, among other things: investigating and taking remedial actions to the fraudulent/suspicious instances of fraud and identity theft identified above; contacting banks and/or credit card companies regarding fraudulent/suspicious activity; investigating and checking the accuracy of the spam and phishing emails, texts, and phone calls she has received and continues to receive on a daily basis; researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter; and monitoring her financial accounts for any indication of additional fraudulent activity on a daily basis.

297. Plaintiff Meyer greatly values her privacy and her Private Information and takes reasonable steps to maintain the confidentiality of her Private Information including, among other things, maintaining strong passwords, regularly changing email and bank passwords, using multi-factor authentication for sensitive accounts, regularly reviewing financial and other important account activity, promptly investigating any alerts about login attempts or suspicious activity, avoiding transactions with businesses she does not trust, storing important documents in a safe place, and making sure that she has not shared her Social Security number publicly or directly to any unknown or untrusted individuals or entities.

298. Despite these efforts, Plaintiff Meyer is very concerned about fraud and identity theft, as well as the consequences of such fraud and identity theft, resulting from the Data Breach. Specifically, the Data Breach has caused Plaintiff Meyer to fear for her personal financial security and suffer stress and anxiety from having to deal with daily spam and fraudulent activity.

299. The daily stress, fear, rage, anger, and time spent by Plaintiff Meyer as a result of the Data Breach has caused and continues to cause Plaintiff Meyer to suffer sleep deprivation, leading her to frequently stay awake until around 4am without sleep. This, in turn, has caused her to suffer from a loss of energy and exhaustion the following day.

300. Plaintiff Meyer anticipates spending additional considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach, especially since she continues to be harassed with spam and phishing attempts and fraudulent efforts to access her Apple account. In addition, Plaintiff Meyer will continue to be at present and continued increased risk of identity theft and fraud for years to come.

301. Plaintiff Meyer has a continuing interest in ensuring that her Private Information, which remains in Progress and Welltok Bellwether Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

302. As a result of the Data Breach, Plaintiff Meyer has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen Private Information, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised Private

Information; and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff Meyer now faces a substantial risk that unauthorized third parties will further misuse her Private Information because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Private Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of Private Information CL0P exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff Meyer's name. As a result of the Data Breach, Plaintiff Meyer has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen Private Information such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her Private Information and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time that she spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

303. Plaintiff Meyer experienced all of the foregoing harm and injury as a direct result of Progress and Welltok Bellwether Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Meyer would compensate her for the foregoing redressable injuries. Further, Plaintiff Meyer seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Progress and Welltok Bellwether Defendants to take steps to monitor for, protect, and/or prevent misuse of her Private Information

accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

5. Plaintiff Christopher Rehm

304. Plaintiff Christopher Rehm ("Plaintiff Rehm") is a resident and citizen of the state of Illinois and resides in Bloomington, Illinois.

305. Plaintiff Rehm is a former patient at OSF, which, according to Plaintiff Rehm's Notice Letter, contracted with Welltok to "operate[] a contact platform for OSF Healthcare and received [Plaintiff Rehm's] [Private Information] in connection with those services."

306. Plaintiff Rehm received a Notice Letter by U.S. mail addressed to him directly from Welltok, writing on behalf of OSF, dated December 4, 2023. According to the Notice Letter, Plaintiff Rehm's Private Information was improperly accessed and obtained by unauthorized third parties, which may have included his "name and Date of Birth, Treatment/Diagnosis."

307. Plaintiff Rehm's Notice Letter states that:

> **What Happened.** On July 26, 2023, we were alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool. We had previously installed all published patches and security upgrades immediately upon such patches being made available by Progress Software, the maker of the MOVEit Transfer tool and conducted an examination of our systems and networks using all information available to determine the potential impact of the published vulnerabilities' presence on the MOVEit Transfer server and the security of data housed on the server and confirmed that there was no indication of any compromise at that time.
>
> Upon being alerted to the alleged issue, we moved quickly to launch an additional investigation with the assistance of third-party cybersecurity specialists and using additional information that had been discovered in the intervening period, to determine the potential for a hidden presence of vulnerabilities' on the MOVEit Transfer server and the security of data housed on the server. After a full reconstruction of our systems and historical data, our investigation determined on August 11, 2023 that an unknown actor exploited software vulnerabilities, accessed the MOVEit Transfer server on May 30, 2023, and exfiltrated certain data from the MOVEit Transfer server during that time. We subsequently undertook a time-consuming and detailed reconstruction and review of the data stored on the server

> at the time of this incident to understand the contents of that data and to whom that data relates. Subsequently, we have learned that data related to you was present on the impacted server at the time of the event.

308. At the time that Progress discovered the Data Breach—on or around July 26, 2023—Welltok and OSF were in possession or and/or had stored Plaintiff Rehm's Private Information but failed to protect it and, instead allowed cybercriminal to access it through the Data Breach. As Plaintiff Rehm's Notice Letter acknowledges, after a "review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data relates[,]" Welltok "learned that data related to you was present on the impacted server at the time of the event."

309. Welltok and OSF also failed to timely and adequately notify Plaintiff Rehm about the Data Breach. Although the Notice Letter disclosed that Welltok had been "alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool," on July 26, 2023, it took Welltok and OSF *over four months* to notify Plaintiff Rehm of the Data Breach's occurrence.

310. In addition to their substantial delay in notifying Plaintiff Rehm of the Data Breach, Welltok and OSF also put the burden on Plaintiff Rehm to prevent any further harm resulting from the Data Breach by not disclosing the specific Private Information of Plaintiff Rehm that was compromised or the specific actions taken by Welltok and OSF in response to the Data Breach.

311. Instead, Plaintiff Rehm's Notice Letter simply identified categories of Plaintiff Rehm's Private Information that may or may not have been compromised by the Data Breach, stating that, "[t]he following types of information may have been impacted: name and Date of Birth, Treatment/Diagnosis."

312. Plaintiff Rehm's Notice Letter further stated vaguely that "we are reviewing and enhancing our existing policies and procedures related to data privacy to reduce the likelihood of a similar future event." The Notice Letter also advised Plaintiff Rehm in general terms "to remain vigilant against incidents of identity theft and fraud by regularly reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

313. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Rehm who retains a vested interest in ensuring that his Private Information remains protected.

314. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff Rehm of the Data Breach's critical facts. Without these details, Plaintiffs Rehm's ability to mitigate the harms resulting from the Data Breach is severely diminished.

315. Plaintiff Rehm's Private Information compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. Since the Data Breach, an unknown person(s) gained access to his telephone number and used it to spoof his number and make telephone calls to people on his contacts list, pretending to be Plaintiff Rehm. The spoofing caused all calls from the unknown person(s) to appear on recipients' caller ID as being from Plaintiff Rehm's telephone when in fact it was not. The unknown caller(s), pretending to be Plaintiff Rehm pretending to call from his telephone number would attempt to scam and illicit money from recipients. While Plaintiff Rehm is unaware of the precise number of people who have been called through this scam, he was made aware of it from numerous such recipients who reported it to him, most recently occurring in late September/early October 2024.

316. As a direct and proximate result of the Data Breach, Plaintiff Rehm has spent substantial time and effort on, among other things: investigating and checking the accuracy of the spam and phishing emails, texts, and phone calls he has received and continues to receive; regularly changing passwords for sensitive accounts such as bank accounts; researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter; monitoring his financial accounts for any indication of additional fraudulent activity on a daily basis; dealing with the ongoing spoofing scam he experienced; and calling Welltok over a dozen times in connection with the Data Breach.

317. Plaintiff Rehm greatly values his privacy and his Private Information and takes reasonable steps to maintain the confidentiality of his Private Information including, among other things, maintaining strong passwords that use the maximum character length and are generated by a random password generator program, encrypting everything he can, regularly changing his email and bank passwords, using multi-factor authentication whenever it is available, regularly reviewing financial and other important account activity, promptly investigating any alerts about login attempts or suspicious activity, avoiding transactions with businesses he does not trust, storing important documents in a safe place, using a well-built shredder to shred important documents, and making sure that he has not shared his social security number publicly or directly to any unknown or untrusted individuals or entities.

318. Despite these efforts, Plaintiff Rehm is very concerned about fraud and identity theft, as well as the consequences of such fraud and identity theft, resulting from the Data Breach. Specifically, the Data Breach has caused Plaintiff Rehm to experience stress, anxiety, and fear, particularly given that he does not what specific information of his was compromised in the Data Breach and given that the spoofing issue he is encountering can result in his personal telephone

number being reported as a spam number that will be automatically blocked by his friends, family, and other contacts. Plaintiff Rehm has also suffered a loss of sleep from stressing over the Data Breach and feelings of helplessness to prevent fraudulent activity and identity theft, including continued spoofing of his telephone number and identity.

319. Plaintiff Rehm anticipates spending additional considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. In addition, Plaintiff Rehm will continue to be at present and continued increased risk of identity theft and fraud for years to come.

320. Plaintiff Rehm has a continuing interest in ensuring that his Private Information, which remains in Progress and Welltok Bellwether Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

321. As a result of the Data Breach, Plaintiff Rehm has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of his stolen Private Information, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of his personal data; lost property in the form of his compromised Private Information; and injury to his privacy. Additionally, as a direct result of the Data Breach, Plaintiff Rehm now faces a substantial risk that unauthorized third parties will further misuse his Private Information because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Private Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized

conduct; and (3) the type of Private Information CL0P exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff Rehm's name. As a result of the Data Breach, Plaintiff Rehm has (1) suffered, or is at an increased risk of suffering, unauthorized use of his stolen Private Information such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his Private Information and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm because his lost time that he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort his expended addressing future consequences of the Data Breach.

322. Plaintiff Rehm experienced all of the foregoing harm and injury as a direct result of Progress and Welltok Bellwether Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Rehm would compensate him for the foregoing redressable injuries. Further, Plaintiff Rehm seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Progress and Welltok Bellwether Defendants to take steps to monitor for, protect, and/or prevent misuse of his Private Information accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

6. Plaintiff Sherrie Rodda

323. Plaintiff Sherrie Rodda ("Plaintiff Rodda") is a resident and citizen of the state of Texas and resides in McKinney, Texas.

324. Plaintiff Rodda is a current patient at Baylor Scott, which, according to Plaintiff Rodda's Notice Letter, contracted with Welltok to "operate[] an online contract-management platform that enables its healthcare clients, including Baylor Scott & White Health, to provide

patients and members with important notices and communications, and received your information in connection with these services."

325. Plaintiff Rodda received a Notice Letter by U.S. mail addressed to her directly from Welltok, writing on behalf of Baylor Scott, dated January 9, 2024. According to the Notice Letter, Plaintiff Rodda's Private Information was improperly accessed and obtained by unauthorized third parties, which may have included her "name and Social Security number, date of birth, health insurance information, MRN/patient id, provider name, treatment cost information, and treatment information/diagnosis."

326. Plaintiff Rodda's Notice Letter states that:

> **What Happened.** On July 26, 2023, we were alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool. We had previously installed all published patches and security upgrades immediately upon such patches being made available by Progress Software, the maker of the MOVEit Transfer tool and conducted an examination of our systems and networks using all information available to determine the potential impact of the published vulnerabilities' presence on the MOVEit Transfer server and the security of data housed on the server and confirmed that there was no indication of any compromise at that time.
>
> Upon being alerted to the alleged issue, we moved quickly to launch an additional investigation with the assistance of third-party cybersecurity specialists and using additional information that had been discovered in the intervening period, to determine the potential for a hidden presence of vulnerabilities' on the MOVEit Transfer server and the security of data housed on the server. After a full reconstruction of our systems and historical data, our investigation determined on August 11, 2023 that an unknown actor exploited software vulnerabilities, accessed the MOVEit Transfer server on May 30, 2023, and exfiltrated certain data from the MOVEit Transfer server during that time. We subsequently undertook a time-consuming and detailed reconstruction and review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data relates. Subsequently, we have learned that data related to you was present on the impacted server at the time of the event.

327. At the time that Progress discovered the Data Breach—on or around May 31, 2023—Welltok and Baylor Scott were in possession and/or had stored Plaintiff Rodda's Private

Information but failed to protect it and, instead allowed cybercriminal to access it through the Data Breach. As Plaintiff Rodda's Notice Letter acknowledges, after a "review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data relates[,]" Welltok "learned that data related to you was present on the impacted server at the time of the event."

328. Welltok and Baylor Scott also failed to timely and adequately notify Plaintiff Rodda about the Data Breach. Although the Notice Letter disclosed that Welltok had been "alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool," on July 26, 2023, it took Welltok *six months* to notify Plaintiff Rodda of the Data Breach's occurrence.

329. In addition to their substantial delay in notifying Plaintiff Rodda of the Data Breach, Welltok and Baylor Scott also put the burden on Plaintiff Rodda to prevent any further harm resulting from the Data Breach by not disclosing the specific Private Information of Plaintiff Rodda that was compromised or the specific actions taken by Welltok and Baylor Scott in response to the Data Breach.

330. Instead, Plaintiff Rodda's Notice Letter simply identified categories of Plaintiff Rodda's Private Information that may or may not have been compromised by the Data Breach, stating that, "[t]he following types of information may have been impacted: "name and Social Security number, date of birth, health insurance information, MRN/patient id, provider name, treatment cost information, and treatment information/diagnosis."

331. Plaintiff Rodda's Notice Letter further stated vaguely that "we are reviewing and enhancing our existing policies and procedures related to data privacy to reduce the likelihood of a similar future event." The Notice Letter also advised Plaintiff Rodda in general terms "to remain

vigilant against incidents of identity theft and fraud by regularly reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

332. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Rodda who retains a vested interest in ensuring that her Private Information remains protected.

333. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff Rodda of the Data Breach's critical facts. Without these details, Plaintiffs Rodda's ability to mitigate the harms resulting from the Data Breach is severely diminished.

334. Plaintiff Rodda's Private Information compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. On or around September 23, 2024, a fraudulent charge was made on Plaintiff Rodda's Citibank card by an unknown person in the amount of approximately $50, causing Plaintiff Rodda to call her bank to cancel the card and close the account and to remove that card from all autopay accounts she had used it for.

335. In addition, since the Data Breach, Plaintiff Rodda received several dozen notifications from ProtectMyID, Chase Credit Journey and Experian, reporting that her Private Information had been found on the Dark Web, including specifically her Social Security number and email. Plaintiff Rodda receives approximately five to six new Dark Web notifications each month.

336. Further, since the Data Breach, Plaintiff Rodda has experienced other forms of spam and phishing emails, texts, and phone calls on a daily basis. This misuse of her Private Information was caused, upon information and belief, by the fact that cybercriminals are able to

easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

337. As a direct and proximate result of the Data Breach, Plaintiff Rodda has spent substantial time (approximately 5-10 hours each week since the Data Breach) and effort on, among other things: constantly checking credit reports, bank accounts, and credit card statements; reviewing and investigating her frequent Dark Web notifications; investigating and taking remedial actions to the authorized credit card purchase and account closure identified above; contacting banks and/or credit card companies regarding fraudulent/suspicious activity; investigating and checking the accuracy of the spam and phishing emails, texts, and phone calls she has received; and researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter.

338. Plaintiff Rodda greatly values her privacy and her Private Information and takes reasonable steps to maintain the confidentiality of her Private Information including, among other things, maintaining strong passwords, using multi-factor authentication for sensitive accounts, regularly reviewing financial and other important account activity, promptly investigating any alerts about login attempts or suspicious activity, avoiding transactions with businesses she does not trust, storing important documents in a safe place, shredding or destroying sensitive documents, and making sure that she has not shared her Social Security number publicly or directly to any unknown or untrusted individuals or entities.

339. Despite these efforts, Plaintiff Rodda is very concerned about fraud and identity theft, as well as the consequences of such fraud and identity theft, resulting from the Data Breach. Specifically, the Data Breach has caused Plaintiff Rodda to fear for her personal financial security and suffer stress and anxiety from knowing through repeated Dark Web notifications that her Social Security number was found on the Dark Web while, at the same time, not knowing if/when she will experience fraudulent activity and/or identity theft as a result.

340. As a result of the Data Breach, Plaintiff Rodda also suffers from sleep disruption each time she receives one of the five to six Dark Web notifications she receives every month.

341. Plaintiff Rodda anticipates spending additional considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach, especially since she continues to be harassed with spam and phishing attempts and Dark Web notifications. In addition, Plaintiff Rodda will continue to be at present and continued increased risk of identity theft and fraud for years to come.

342. Plaintiff Rodda has a continuing interest in ensuring that her Private Information, which remains in Progress and Welltok Bellwether Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

343. As a result of the Data Breach, Plaintiff Rodda has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen Private Information, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised Private

Information; and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff Rodda now faces a substantial risk that unauthorized third parties will further misuse her Private Information because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Private Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of Private Information CL0P exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff Rodda's name. As a result of the Data Breach, Plaintiff Rodda has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen Private Information such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her Private Information and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time that she spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

344. Plaintiff Rodda experienced all of the foregoing harm and injury as a direct result of Progress and Welltok Bellwether Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Rodda would compensate her for the foregoing redressable injuries. Further, Plaintiff Rodda seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Progress and Welltok Bellwether Defendants to take steps to monitor for, protect, and/or prevent misuse of her Private Information

accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

7. Plaintiff Laquesha George

345. Plaintiff Laquesha George ("Plaintiff George") is a resident and citizen of the state of Nebraska and resides in Omaha, Nebraska.

346. Plaintiff George is a current patient at CHI, which, according to Plaintiff George's Notice Letter, contracted with Welltok to "operate[] an online contract-management platform that enables healthcare clients to provide patients and members with important notices and communications for CHI Health - NE and received your information in connection with these services."

347. Plaintiff George received a Notice Letter by U.S. mail addressed to her directly from Welltok, writing on behalf of CHI, dated December 1, 2023. According to the Notice Letter, Plaintiff George's Private Information was improperly accessed and obtained by unauthorized third parties, which may have included her "name and [sic] name, address, date of birth, some clinical information, patient ID, and health insurance information."

348. Plaintiff George's Notice Letter states that:

> **What Happened.** On July 26, 2023, we were alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool. We had previously installed all published patches and security upgrades immediately upon such patches being made available by Progress Software, the maker of the MOVEit Transfer tool and conducted an examination of our systems and networks using all information available to determine the potential impact of the published vulnerabilities' presence on the MOVEit Transfer server and the security of data housed on the server and confirmed that there was no indication of any compromise at that time.
>
> Upon being alerted to the alleged issue, we moved quickly to launch an additional investigation with the assistance of third-party cybersecurity specialists and using additional information that had been discovered in the intervening period, to determine the potential for a hidden presence of vulnerabilities' on the MOVEit

> Transfer server and the security of data housed on the server. After a full reconstruction of our systems and historical data, our investigation determined on August 11, 2023 that an unknown actor exploited software vulnerabilities, accessed the MOVEit Transfer server on May 30, 2023, and exfiltrated certain data from the MOVEit Transfer server during that time. We subsequently undertook a time-consuming and detailed reconstruction and review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data relates. Subsequently, we have learned that data related to you was present on the impacted server at the time of the event.

349. At the time that Progress discovered the Data Breach—on or around May 31, 2023—Welltok and CHI were in possession or and/or had stored Plaintiff George's Private Information but failed to protect it and, instead allowed cybercriminal to access it through the Data Breach. As Plaintiff George's Notice Letter acknowledges, after a "review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data relates[,]" Welltok "learned that data related to you was present on the impacted server at the time of the event."

350. Welltok and CHI also failed to timely and adequately notify Plaintiff George about the Data Breach. Although the Notice Letter disclosed that Welltok had been "alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool," on July 26, 2023, it took Welltok and CHI *over four months* to notify Plaintiff George of the Data Breach's occurrence.

351. In addition to their substantial delay in notifying Plaintiff George of the Data Breach, Welltok and CHI also put the burden on Plaintiff George to prevent any further harm resulting from the Data Breach by not disclosing the specific Private Information of Plaintiff George that was compromised or the specific actions taken by Welltok and CHI in response to the Data Breach.

352. Instead, Plaintiff George's Notice Letter simply identified categories of Plaintiff George's Private Information that may or may not have been compromised by the Data Breach, stating that, "[t]he following types of information may have been impacted: name and [sic] name, address, date of birth, some clinical information, patient ID, and health insurance information."

353. Plaintiff George's Notice Letter further stated vaguely that "we are reviewing and enhancing our existing policies and procedures related to data privacy to reduce the likelihood of a similar future event." The Notice Letter also advised Plaintiff George in general terms "to remain vigilant against incidents of identity theft and fraud by regularly reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

354. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff George who retains a vested interest in ensuring that her Private Information remains protected.

355. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff George of the Data Breach's critical facts. Without these details, Plaintiff George's ability to mitigate the harms resulting from the Data Breach is severely diminished.

356. Plaintiff George's Private Information compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. Since the Data Breach, Plaintiff George started receiving repeated telephone calls and voicemail messages from an unknown person(s) calling from an unknown phone number demanding that Plaintiff George confirm her identity by proving her Private Information. These calls and voicemail have recently become more threatening in nature, as the caller has threatened to physically come to Plaintiff George's home if

she does not provide her Private Information to him over the phone. These calls have continued into October 2024.

357. In addition, since the Data Breach, Plaintiff George has experienced other forms of spam and phishing emails, texts, and phone calls on a daily basis. This misuse of her Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

358. As a direct and proximate result of the Data Breach, Plaintiff George has spent substantial time and effort on, among other things: investigating and handling the frequent spam and phishing calls and voicemails she receives and the threats made in connection with those calls; checking the accuracy of other spam and phishing emails, texts, and phone calls she receives; checking credit reports, bank accounts, and credit card statements; and investigating and researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter.

359. Plaintiff George greatly values her privacy and her Private Information and takes reasonable steps to maintain the confidentiality of her Private Information including, among other things, maintaining strong passwords, using multi-factor authentication for sensitive accounts, regularly reviewing financial and other important account activity, promptly investigating any alerts about login attempts or suspicious activity, avoiding transactions with businesses she does not trust, storing important documents in a safe place, shredding sensitive documents, and making

sure that she has not shared her Social Security number publicly or directly to any unknown or untrusted individuals or entities.

360. Despite these efforts, Plaintiff George is very concerned about fraud and identity theft, as well as the consequences of such fraud and identity theft, resulting from the Data Breach. Specifically, the Data Breach has caused Plaintiff George to fear for her personal financial security and the personal safety of her and her family due to the harassing and threatening phishing calls she receives demanding that she provides her Private Information. Plaintiff George has also suffered a frequent sleep disruption from late night checking bank and credit card statements for fraudulent activity and dealing with late night spam calls she receives. Plaintiff George further fears that someone will use her Private Information or steal her identity since her private Information was compromised. The Data Breach has caused Plaintiff George daily stress, anxiety, anger, and fear.

361. Plaintiff George anticipates spending additional considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach, especially since she continues to be harassed with spam and phishing attempts. In addition, Plaintiff George will continue to be at present and continued increased risk of identity theft and fraud for years to come.

362. Plaintiff George has a continuing interest in ensuring that her Private Information, which remains in Progress and Welltok Bellwether Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

363. As a result of the Data Breach, Plaintiff George has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen Private Information, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft; time and expenses spent

scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised Private Information; and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff George now faces a substantial risk that unauthorized third parties will further misuse her Private Information because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Private Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of Private Information CL0P exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff George's name. As a result of the Data Breach, Plaintiff George has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen Private Information such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her Private Information and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time that she spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

364. Plaintiff George experienced all of the foregoing harm and injury as a direct result of Progress and Welltok Bellwether Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff George would compensate her for the foregoing redressable injuries. Further, Plaintiff George seeks injunctive relief to redress the foregoing

injuries and harm, including, but not limited to, requiring Progress and Welltok Bellwether Defendants to take steps to monitor for, protect, and/or prevent misuse of her Private Information accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

8. Plaintiff Megan McClendon

365. Plaintiff Megan McClendon ("Plaintiff McClendon") is a resident and citizen of the state of Washington and resides in Lakewood, Washington.

366. Plaintiff McClendon is a current patient at Virginia Mason, which, according to Plaintiff McClendon's Notice Letter, contracted with Welltok to "operate[] an online contract-management platform that enables healthcare clients to provide patients and members with important notices and communications for Virginia Mason Franciscan Health and received your information in connection with these services."

367. Plaintiff McClendon received a Notice Letter by U.S. mail addressed to her directly from Welltok, writing on behalf of Virginia Mason, dated December 1, 2023. According to the Notice Letter, Plaintiff McClendon's Private Information was improperly accessed and obtained by unauthorized third parties, which may have included her "name, address, date of birth, some clinical information, patient ID, and health insurance information."

368. Plaintiff McClendon's Notice Letter states that:

> **What Happened.** On July 26, 2023, we were alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool. We had previously installed all published patches and security upgrades immediately upon such patches being made available by Progress Software, the maker of the MOVEit Transfer tool and conducted an examination of our systems and networks using all information available to determine the potential impact of the published vulnerabilities' presence on the MOVEit Transfer server and the security of data housed on the server and confirmed that there was no indication of any compromise at that time.

> Upon being alerted to the alleged issue, we moved quickly to launch an additional investigation with the assistance of third-party cybersecurity specialists and using additional information that had been discovered in the intervening period, to determine the potential for a hidden presence of vulnerabilities' on the MOVEit Transfer server and the security of data housed on the server. After a full reconstruction of our systems and historical data, our investigation determined on August 11, 2023 that an unknown actor exploited software vulnerabilities, accessed the MOVEit Transfer server on May 30, 2023, and exfiltrated certain data from the MOVEit Transfer server during that time. We subsequently undertook a time-consuming and detailed reconstruction and review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data relates. Subsequently, we have learned that data related to you was present on the impacted server at the time of the event.

369. At the time that Progress discovered the Data Breach—on or around May 31, 2023—Welltok and Virginia Mason were in possession and/or had stored Plaintiff McClendon's Private Information but failed to protect it and, instead allowed cybercriminal to access it through the Data Breach. As Plaintiff McClendon's Notice Letter acknowledges, after a "review of the data stored on the server at the time of this incident to understand the contents of that data and to whom that data relates[,]" Welltok "learned that data related to you was present on the impacted server at the time of the event."

370. Welltok and Virginia Mason also failed to timely and adequately notify Plaintiff McClendon about the Data Breach. Although the Notice Letter disclosed that Welltok had been "alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool," on July 26, 2023, it took Welltok and Virginia Mason over four months to notify Plaintiff McClendon of the Data Breach's occurrence.

371. In addition to their substantial delay in notifying Plaintiff McClendon of the Data Breach, Welltok and Virginia Mason also put the burden on Plaintiff McClendon to prevent any further harm resulting from the Data Breach by not disclosing the specific Private Information of

Plaintiff McClendon that was compromised or the specific actions taken by Welltok and Virginia Mason in response to the Data Breach.

372. Instead, Plaintiff McClendon's Notice Letter simply identified categories of Plaintiff McClendon's Private Information that may or may not have been compromised by the Data Breach, stating that, "[t]he following types of information may have been impacted: name, address, date of birth, some clinical information, patient ID, and health insurance information."

373. Plaintiff McClendon's Notice Letter further stated vaguely that "we are reviewing and enhancing our existing policies and procedures related to data privacy to reduce the likelihood of a similar future event." The Notice Letter also advised Plaintiff McClendon in general terms "to remain vigilant against incidents of identity theft and fraud by regularly reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

374. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff McClendon who retains a vested interest in ensuring that her Private Information remains protected.

375. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff McClendon of the Data Breach's critical facts. Without these details, Plaintiffs McClendon's ability to mitigate the harms resulting from the Data Breach is severely diminished.

376. Plaintiff McClendon's Private Information compromised in the Data Breach has already been circulated on the Dark Web. Indeed, Plaintiff McClendon has received several notifications from IDNotify in 2024, most recently on September 23, 2024, reporting that her Private Information was found on the Dark Web.

377. In addition, since the Data Breach, Plaintiff McClendon has experienced other forms of spam and phishing emails, texts, and phone calls on a daily basis. This misuse of her Private Information was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

378. As a result of the Data Breach, Plaintiff McClendon pays $100 annually in out-of-pocket costs for credit monitoring services with IDNotify.

379. As a direct and proximate result of the Data Breach, Plaintiff McClendon has spent substantial time and effort on, among other things: investigating and handling the frequent spam and phishing emails, texts, and calls she receives; checking credit reports, bank accounts, and credit card statements; and investigating, researching, and verifying the legitimacy of the Data Breach upon receiving the Notice Letter.

380. Plaintiff McClendon greatly values her privacy and her Private Information and takes reasonable steps to maintain the confidentiality of her Private Information including, among other things, using credit monitoring services for which she pays an annual fee, maintaining strong passwords and not using the same password for more than one account, using multi-factor authentication for sensitive accounts, regularly reviewing financial and other important account activity, promptly investigating any alerts about login attempts or suspicious activity, avoiding transactions with businesses she does not trust, storing important documents in a safe place,

keeping important/sensitive documents locked up for safe keeping, and making sure that she has not shared her Social Security number publicly or directly to any unknown or untrusted individuals or entities.

381. Despite these efforts, Plaintiff McClendon is very concerned about fraud and identity theft, as well as the consequences of such fraud and identity theft, resulting from the Data Breach. Specifically, she suffers daily stress and anxiety and fears what Private Information of hers is on the Dark Web and how it might be used to engage in fraudulent activity and identity theft and to damage her credit. Plaintiff McClendon is angry over Welltok and Virginia Mason not adequately safeguarding her Private Information. In addition, Plaintiff McClendon has suffered from sleep disruption and frequent nightmares from stressing over what Private Information of hers is in the hands of criminals and what they could do with that Private Information. This stress, anxiety, and sleep disruption has recently caused Plaintiff McClendon to experience stress-related hair loss.

382. Plaintiff McClendon anticipates spending additional considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff McClendon will continue to be at present and continued increased risk of identity theft and fraud for years to come.

383. Plaintiff McClendon has a continuing interest in ensuring that her Private Information, which remains in Progress and Welltok Bellwether Defendants' possession, is protected and safeguarded from future disclosure and/or data breaches.

384. As a result of the Data Breach, Plaintiff McClendon has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen Private Information, heightened threat of identity theft and general

mitigation efforts spent on monitoring her credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised Private Information; and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff McClendon now faces a substantial risk that unauthorized third parties will further misuse her Private Information because (1) the Data Breach involved a single cybercriminal organization, CL0P, specifically targeting Defendants' systems; (2) the dataset of Private Information that CL0P exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of Private Information CL0P exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff McClendon's name. As a result of the Data Breach, Plaintiff McClendon has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen Private Information such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her Private Information and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time that she spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

385. Plaintiff McClendon experienced all of the foregoing harm and injury as a direct result of Progress and Welltok Bellwether Defendants' actions and inactions that led to the Data Breach. TPhe monetary relief sought herein by Plaintiff McClendon would compensate her for the

foregoing redressable injuries. Further, Plaintiff McClendon seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Progress and Welltok Bellwether Defendants to take steps to monitor for, protect, and/or prevent misuse of her Private Information accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

C. Delta Dental Bellwether Plaintiffs

1. Karen Boginski

386. Plaintiff Karen Boginski is, and at all times mentioned herein was, an individual citizen of the State of Connecticut, residing in Stamford, Connecticut.

387. Plaintiff is a current customer of DDIC and was a customer at the time of the Data Breach. Plaintiff receives Delta Dental insurance through her spouse's employer.

388. Plaintiff Boginski provided her Private Information to Delta Dental Bellwether Defendants as a condition of receiving dental insurance.

389. Plaintiff Boginski had the reasonable expectation and understanding that Delta Dental Bellwether Defendants would take—at minimum—industry standard precautions to protect, maintain, and safeguard that highly sensitive information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff would not have entrusted her Private Information to Delta Dental Bellwether Defendants had she known that Delta Dental Bellwether Defendants would not take reasonable steps to safeguard her information.

390. Plaintiff Boginski received a letter from "Delta Dental of California and affiliates" (referred to in the Notice Letter as "Company") dated January 19, 2024 concerning the Data Breach. The letter explained that cybercriminals exploited a security vulnerability in the systems of one of Delta Dental of California and affiliates' third-party vendors, Progress. As a result,

unauthorized individuals accessed or obtained data stored on the platform, including the Plaintiff's information. The letter further states the following:

> **What Happened?**
>
> Progress Software announced a previously unknown vulnerability within their widely used MOVEit file-transfer software program. This vulnerability led to a global data security incident that is reported to have impacted many organizations, including corporations, government agencies, insurance providers, pension funds, financial institutions, state education systems and more. On June 1, 2023, the Company learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application. Immediately after being alerted of the incident, we launched a thorough investigation and took steps to contain and remediate the incident. We stopped access to the MOVEit software, removed the malicious files, conducted a thorough analysis of the MOVEit database, applied the recommended patches, and reset administrative passwords to the MOVEit system. We also enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity, and ransomware activity. On July 6, 2023, our investigation confirmed that the Company information on the MOVEit platform had been accessed and acquired without authorization between May 27, 2023 and May 30, 2023. At that time, we promptly engaged independent third-party experts in computer forensics, analytics, and data mining to determine what information was impacted and with whom it is associated. This extensive investigation and analysis of the data recently concluded and was a critical component in enabling us to identify specific personal information that was acquired from the MOVEit platform. Upon that determination, we have worked diligently to identify any impacted individuals to provide notification. On November 27, 2023, we determined your personal information was affected. In addition to our own investigation, we have also notified law enforcement of the incident and have been cooperating with them since.
>
> **What Information Was Involved?** Your affected information included date of birth, Social Security number, and health insurance information.

391. Since the Data Breach, including prior to being notified by Delta Dental of California and affiliates that her Private Information had been compromised and in the hands of cybercriminals, Plaintiff has experienced an increase in the amount of intrusive spam calls, texts, and emails she receives. She has also received alerts that her Private Information was found on the dark web since the Data Breach occurred.

392. As a result of the Data Breach, Plaintiff Boginski purchased the credit monitoring service, BitDefender, for an annual fee of $99.

393. As a result of the Data Breach, she will have to maintain a subscription to Deleteme.com to control the proliferation of her personal data to data brokers, for an annual fee of $129.

394. Upon information and belief, Plaintiff Boginski's unencrypted Private Information was viewed by unauthorized persons, as evidenced by the fact that Plaintiff has experienced an uptick in phishing emails since the Data Breach and the notifications she received that her information was listed on the dark web, among other harms described.

395. The disclosure of her health insurance information is highly offensive due to the deeply personal nature of health and medical data. This Data Breach has caused her significant anxiety, increased concerns about the loss of privacy, and fears over the potential misuse of her sensitive information by cybercriminals. She now faces a serious risk of identity theft, credit fraud, and other potential harms, both at present and in the future.

396. Plaintiff Boginski values her privacy and is very careful about storing and sharing sensitive Private Information. Plaintiff would not have entrusted her Private Information to Delta Dental Bellwether Defendants had she known of their inadequate and lax data security policies and practices.

397. Plaintiff Boginski has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Delta Dental of California and affiliates' possession, is protected and safeguarded from future breaches.

398. As a direct and proximate result of the Data Breach, Plaintiff Boginski has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely

monitoring her financial accounts, investigating fraudulent and suspicious activity to reduce the risk of future identity theft and fraud, as well as purchasing credit monitoring services, actively monitoring her credit, and contacting major credit bureaus to freeze her credit.

399. To date, as a result of the Data Breach, Plaintiff Boginski has expended over fifteen hours between researching the details of the Data Breach and her efforts trying to mitigate the harms of the Data Breach, as described, which are practices that she will need to continue indefinitely to protect against and/or remedy fraud and identity theft.

400. Had Delta Dental of California and affiliates not delayed in notifying Plaintiff Boginski about the Data Breach, she could have taken additional precautions earlier on to protect her identity and mitigate the harms of the Data Breach.

401. As a result of the Data Breach, Plaintiff Boginski anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She has faced and continues to face a risk of fraud and identity theft that will last for her lifetime.

402. Plaintiff Boginski suffered lost time, annoyance, interference, and inconvenience, as well as money from purchasing credit monitoring services, as a result of the Data Breach.

403. Had Plaintiff Boginski been informed that Delta Dental Bellwether Defendants had insufficient data security measures to protect her Private Information, she would have taken this into account in deciding whether to enroll in Delta Dental insurance, and, at a minimum, Plaintiff would not have paid as much for dental insurance.

404. Plaintiff Boginski relied on Delta Dental Bellwether Defendants' policies and promises to implement sufficient regulatory and industry compliant measures to protect her Private Information and privacy rights.

405. Due to the highly sensitive nature of the stolen information and its unauthorized dissemination, Plaintiff has already suffered harm, including damages and a loss in the value of her Private Information—an intangible asset entrusted to the Delta Dental Bellwether Defendants. Plaintiff also faces a substantial and imminent risk of future harm.

2. Doris Cadet

406. Plaintiff Doris Cadet is, and at all times mentioned herein was, an individual citizen of the State of Georgia, residing in Riverdale, Georgia.

407. Plaintiff Cadet is a current customer of DDIC and was a customer at the time of the Data Breach. Plaintiff receives Delta Dental insurance through her employer.

408. Plaintiff Cadet provided her Private Information to Delta Dental Bellwether Defendants as a condition of receiving dental insurance.

409. Plaintiff Cadet had the reasonable expectation and understanding that Delta Dental Bellwether Defendants would take—at minimum—industry standard precautions to protect, maintain, and safeguard that highly sensitive information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff would not have entrusted her Private Information to DDCA and Affiliates had she known that DDCA and Affiliates would not take reasonable steps to safeguard her information.

410. Plaintiff Cadet received a letter from "Delta Dental of California and affiliates" dated on or after December 15, 2023 concerning the Data Breach. The letter explained that cybercriminals exploited a security vulnerability in the systems of one of Delta Dental of California and affiliates' third-party vendors, Progress. As a result, unauthorized individuals accessed or obtained data stored on the platform, including the Plaintiff's information. The letter further states the following:

What Happened?

Progress Software announced a previously unknown vulnerability within their widely used MOVEit file-transfer software program. This vulnerability led to a global data security incident that is reported to have impacted many organizations, including corporations, government agencies, insurance providers, pension funds, financial institutions, state education systems and more. On June 1, 2023, the Company learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application. Immediately after being alerted of the incident, we launched a thorough investigation and took steps to contain and remediate the incident. We stopped access to the MOVEit software, removed the malicious files, conducted a thorough analysis of the MOVEit database, applied the recommended patches, and reset administrative passwords to the MOVEit system. We also enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity, and ransomware activity. On July 6, 2023, our investigation confirmed that the Company information on the MOVEit platform had been accessed and acquired without authorization between May 27, 2023 and May 30, 2023. At that time, we promptly engaged independent third-party experts in computer forensics, analytics, and data mining to determine what information was impacted and with whom it is associated. This extensive investigation and analysis of the data recently concluded and was a critical component in enabling us to identify specific personal information that was acquired from the MOVEit platform. Upon that determination, we have worked diligently to identify any impacted individuals to provide notification. On November 27, 2023, we determined your personal information was affected. In addition to our own investigation, we have also notified law enforcement of the incident and have been cooperating with them since.

What Information Was Involved? Your affected information included date of birth, Social Security number, and health insurance information.

411. Since the Data Breach, including prior to being notified by Delta Dental of California and affiliates that her Private Information had been compromised and in the hands of cybercriminals, Plaintiff has experienced an increase in the amount of intrusive spam calls, texts, and emails she receives.

412. Since the Data Breach, Plaintiff Cadet received a notice that a loan she applied to was denied, but neither she nor anyone in her family had applied for a car loan. She also experienced hard inquiries into her credit history.

413. As a consequence of the fraudulent activity subsequent to the Breach, Plaintiff incurred $300 in costs to have her credit repaired.

414. Upon information and belief, Plaintiff's unencrypted Private Information was viewed by unauthorized persons, as evidenced by the fraudulent activity to her credit, the suspicious application for a car loan in her name, and the fact that Plaintiff experienced an uptick in phishing emails since the Data Breach, among other harms described.

415. The disclosure of her health insurance information is highly offensive due to the deeply personal nature of health and medical data. This Data Breach has caused her significant anxiety, increased concerns about the loss of privacy, and fears over the potential misuse of her sensitive information by cybercriminals. She now faces a serious risk of identity theft, credit fraud, and other potential harms, both at present and in the future.

416. Plaintiff Cadet values her privacy and is very careful about storing and sharing sensitive Private Information. Plaintiff would not have entrusted her Private Information to Delta Dental Bellwether Defendants had she known of their inadequate and lax data security policies and practices.

417. Plaintiff Cadet has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Delta Dental of California and affiliates' possession, is protected and safeguarded from future breaches.

418. As a direct and proximate result of the Data Breach, Plaintiff Cadet has made reasonable efforts to mitigate the impact of the Data Breach, including by investigating fraudulent and suspicious activity she experienced, contacting banks, credit card companies, or other vendors about the suspicious, fraudulent activity she experienced, and by regularly and closely monitoring her financial accounts to reduce the risk of future identity theft and fraud.

419. To date, as a result of the Data Breach, Plaintiff Cadet has spent several hours researching the details of the Data Breach and performing those mitigation tasks.

420. Had Delta Dental of California and affiliates not delayed in notifying Plaintiff about the Data Breach, she could have taken additional precautions earlier on to protect her identity and mitigate the harms of the Data Breach.

421. As a result of the Data Breach, Plaintiff Cadet anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. For example, she will need to continue indefinitely to expend time and effort checking her credit and financial accounts for any unauthorized, suspicious activity to protect against and/or remedy fraud and identity theft.

422. She has faced and continues to face a risk of fraud and identity theft that will last for her lifetime.

423. Plaintiff Cadet suffered lost time, annoyance, interference, and inconvenience, as well as money from needing to purchase credit repair services as a result of the Data Breach.

424. Had Plaintiff Cadet been informed that Delta Dental Bellwether Defendants had insufficient data security measures to protect her Private Information, she would have taken this into account in deciding whether to enroll in Delta Dental insurance, and, at a minimum, Plaintiff would not have paid as much for dental insurance.

425. Plaintiff Cadet relied on Delta Dental Bellwether Defendants' policies and promises to implement sufficient regulatory and industry compliant measures to protect her Private Information and privacy rights.

426. Due to the highly sensitive nature of the stolen information and its unauthorized dissemination, Plaintiff has already suffered harm, including damages and a loss in the value of

her Private Information—an intangible asset entrusted to the Delta Dental Bellwether Defendants. Plaintiff also faces a substantial and imminent risk of future harm.

3. Marvin Dovberg

427. Plaintiff Marvin Dovberg is, and at all times mentioned herein was, an individual citizen of the State of Pennsylvania, residing in Huntingdon Valley, Pennsylvania.

428. Plaintiff was a customer of DDPenn at the time of the Data Breach. Plaintiff received Delta Dental insurance through his employer.

429. Plaintiff Dovberg provided his Private Information to Delta Dental Bellwether Defendants as a condition of receiving dental insurance.

430. Plaintiff Dovberg had the reasonable expectation and understanding that Delta Dental Bellwether Defendants would take—at minimum—industry standard precautions to protect, maintain, and safeguard that highly sensitive information from unauthorized users or disclosure, and would timely notify him of any data security incidents. Plaintiff would not have entrusted his Private Information to Delta Dental Bellwether Defendants had he known that Delta Dental Bellwether Defendants would not take reasonable steps to safeguard his information.

431. Plaintiff Dovberg received a letter from "Delta Dental of California and affiliates" (referred to in the Notice Letter as "Company") dated February 9, 2024 concerning the Data Breach. The letter explained that cybercriminals exploited a security vulnerability in the systems of one of Delta Dental of California and affiliates' third-party vendors, Progress. As a result, unauthorized individuals accessed or obtained data stored on the platform, including the Plaintiff's information. The letter further states the following:

> **What Happened?**
>
> Progress Software announced a previously unknown vulnerability within their widely used MOVEit file-transfer software program. This vulnerability led to a global data security incident that is reported to have impacted many organizations,

> including corporations, government agencies, insurance providers, pension funds, financial institutions, state education systems and more. On June 1, 2023, the Company learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application. Immediately after being alerted of the incident, we launched a thorough investigation and took steps to contain and remediate the incident. We stopped access to the MOVEit software, removed the malicious files, conducted a thorough analysis of the MOVEit database, applied the recommended patches, and reset administrative passwords to the MOVEit system. We also enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity, and ransomware activity. On July 6, 2023, our investigation confirmed that the Company information on the MOVEit platform had been accessed and acquired without authorization between May 27, 2023 and May 30, 2023. At that time, we promptly engaged independent third-party experts in computer forensics, analytics, and data mining to determine what information was impacted and with whom it is associated. This extensive investigation and analysis of the data recently concluded and was a critical component in enabling us to identify specific personal information that was acquired from the MOVEit platform. Upon that determination, we have worked diligently to identify any impacted individuals to provide notification. On November 27, 2023, we determined your personal information was affected. In addition to our own investigation, we have also notified law enforcement of the incident and have been cooperating with them since.
>
> **What Information Was Involved?** Y%%our affected information included date of birth and health insurance information**.**

432. Since the Data Breach, including prior to being notified by Delta Dental of California and affiliates that his Private Information had been compromised and in the hands of cybercriminals, Plaintiff has experienced an increase in the amount of intrusive spam calls, texts, and emails he receives.

433. Since the Data Breach, Plaintiff Dovberg discovered fraudulent attempted and/or successful charges on his credit cards, debit cards, or bank accounts.

434. Upon information and belief, Plaintiff Dovberg's unencrypted Private Information was viewed by unauthorized persons, as evidenced by the fraudulent charges and the fact he has experienced an uptick in phishing emails since the Data Breach, among other harms described.

435. The disclosure of his health insurance information is highly offensive due to the deeply personal nature of health and medical data. This Data Breach has caused him significant

anxiety, increased concerns about the loss of privacy, and fears over the potential misuse of his sensitive information by cybercriminals. He now faces a serious risk of identity theft, credit fraud, and other potential harms, both at present and in the future.

436. Plaintiff Dovberg values his privacy and is very careful about storing and sharing sensitive Private Information. Plaintiff would not have entrusted his Private Information to Delta Dental Bellwether Defendants had he known of their inadequate and lax data security policies and practices.

437. Plaintiff Dovberg has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Delta Dental of California and affiliates' possession, is protected and safeguarded from future breaches.

438. As a direct and proximate result of the Data Breach, Plaintiff Dovberg has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring his financial accounts for fraudulent, suspicious, unauthorized activity to reduce the risk of future identity theft and fraud.

439. To date, as a result of the Data Breach, Plaintiff Dovberg has spent several hours researching the details of the Data Breach. Plaintiff has also expended time and effort checking his credit and financial accounts for any unauthorized, suspicious activity, a practice that Plaintiff Dovberg will need to continue indefinitely to protect against and/or remedy fraud and identity theft.

440. Had Delta Dental of California and affiliates not delayed in notifying Plaintiff Dovberg about the Data Breach, he could have taken additional precautions earlier on to protect his identity and mitigate the harms of the Data Breach.

441. As a result of the Data Breach, Plaintiff Dovberg anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. He has faced and continues to face a risk of fraud and identity theft that will last for his lifetime.

442. Plaintiff Dovberg suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

443. Had Plaintiff Dovberg been informed that Delta Dental Bellwether Defendants had insufficient data security measures to protect his Private Information, he would have taken this into account in deciding whether to enroll in Delta Dental insurance, and, at a minimum, Plaintiff would not have paid as much for dental insurance.

444. Plaintiff Dovberg relied on Delta Dental Bellwether Defendants' policies and promises to implement sufficient regulatory and industry compliant measures to protect his Private Information and privacy rights.

445. Due to the highly sensitive nature of the stolen information and its unauthorized dissemination, Plaintiff has already suffered harm, including damages and a loss in the value of her Private Information—an intangible asset entrusted to the Delta Dental Bellwether Defendants. Plaintiff also faces a substantial and imminent risk of future harm.

4. Deanna Duarte

446. Plaintiff Deanna Duarte is, and at all times mentioned herein was, an individual citizen of the State of California, residing in Sacramento, California.

447. Plaintiff Duarte is a current customer of DDCA and was a customer at the time of the Data Breach. She receives her Delta Dental insurance coverage through her employer.

448. Plaintiff Duarte provided her Private Information to Delta Dental Bellwether Defendants as a condition of receiving dental insurance.

449. Plaintiff Duarte had the reasonable expectation and understanding that Delta Dental Bellwether Defendants would take—at minimum—industry standard precautions to protect, maintain, and safeguard that highly sensitive information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff would not have entrusted her Private Information to Delta Dental Bellwether Defendants had she known that they would not take reasonable steps to safeguard her information.

450. On January 10, 2024, Plaintiff Duarte received a letter from "Delta Dental of California and affiliates" regarding the Data Breach (referred to in the Notice Letter as "Company"). The letter explained that cybercriminals exploited a security vulnerability in the systems of one of Delta Dental of California and affiliates' third-party vendors, Progress. As a result, unauthorized individuals accessed or obtained data stored on the platform, including the Plaintiff's information. The letter further states the following:

> **What Happened?**
>
> Progress Software announced a previously unknown vulnerability within their widely used MOVEit file-transfer software program. This vulnerability led to a global data security incident that is reported to have impacted many organizations, including corporations, government agencies, insurance providers, pension funds, financial institutions, state education systems and more. On June 1, 2023, the Company learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application. Immediately after being alerted of the incident, we launched a thorough investigation and took steps to contain and remediate the incident. We stopped access to the MOVEit software, removed the malicious files, conducted a thorough analysis of the MOVEit database, applied the recommended patches, and reset administrative passwords to the MOVEit system. We also enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity, and ransomware activity. On July 6, 2023, our investigation confirmed that the Company information on the MOVEit platform had been accessed and acquired without authorization between May 27, 2023 and May 30, 2023. At that time, we promptly engaged independent third-party experts in computer forensics, analytics, and data mining to determine what information was impacted and with whom it is associated. This extensive investigation and analysis of the data recently concluded and was a critical component in enabling us to identify specific personal information that was acquired from the MOVEit platform. Upon that determination, we have worked

> diligently to identify any impacted individuals to provide notification. On November 27, 2023, we determined your personal information was affected. In addition to our own investigation, we have also notified law enforcement of the incident and have been cooperating with them since.
>
> **What Information Was Involved?** Your affected information included date of birth, Social Security number, and health insurance information.

451. Since the Data Breach, including prior to being notified by Delta Dental of California and affiliates that her Private Information had been compromised and in the hands of cybercriminals, Plaintiff has experienced an increase in the amount of intrusive spam calls, texts, and emails she receives. On or about February 2024, two unknown P.O. boxes were added to her Amazon account that she did not authorize.

452. Upon information and belief, Plaintiff's unencrypted Private Information was viewed by unauthorized persons, as evidenced by the fact that Plaintiff has experienced an uptick in phishing emails since the Data Breach and the notifications she received that her information was listed on the dark web, among other harms described.

453. The disclosure of her health insurance information is highly offensive due to the deeply personal nature of health and medical data. This Data Breach has caused her significant anxiety, heightened concerns over the loss of privacy, and fears about the misuse of her sensitive information by cybercriminals. She now faces an increased risk of identity theft, fraud affecting her credit, and other potential harms, both at present and in the future.

454. Plaintiff Duarte values her privacy and is very careful about storing and sharing sensitive Private Information. Plaintiff would not have entrusted her Private Information to Delta Dental Bellwether Defendants had she known of their inadequate and lax data security policies and practices.

455. Plaintiff Duarte has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Delta Dental Bellwether Defendants' possession is protected and safeguarded from future breaches.

456. As a direct and proximate result of the Data Breach, Plaintiff Duarte has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her financial accounts for suspicious activity to reduce the risk of future identity theft and fraud.

457. To date, as a result of the Data Breach, Plaintiff Duarte has spent several hours researching the details of the Data Breach and has even contacted Delta Dental directly to inquire about the breach, given the inadequate information provided to her.

458. Had Delta Dental of California and affiliates not delayed in notifying Plaintiff about the Data Breach, she could have taken additional precautions earlier on to protect her identity and mitigate the harms of the Data Breach.

459. Plaintiff Duarte has also spent several hours monitoring and investigating fraudulent and suspicious activity, as well as contacting banks, credit card companies, or other vendors about suspicious, fraudulent activity, all of which are practices that Plaintiff Duarte will need to continue indefinitely to protect against and/or remedy fraud and identity theft.

460. As a result of the Data Breach, Plaintiff Duarte anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She has faced and continues to face a risk of fraud and identity theft that will last for her lifetime.

461. Plaintiff Duarte suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

462. Had Plaintiff Duarte been informed that Delta Dental Bellwether Defendants had insufficient data security measures to protect her Private Information, she would have taken this into account in deciding whether to enroll in Delta Dental insurance, and, at a minimum, Plaintiff Duarte would not have paid as much for dental insurance.

463. Plaintiff Duarte relied on Delta Dental Bellwether Defendants' policies and promises to implement sufficient regulatory and industry compliant measures to protect her Private Information and privacy rights.

464. Due to the highly sensitive nature of the stolen information and its unauthorized dissemination, Plaintiff Duarte has already suffered harm, including damages and a loss in the value of her Private Information—an intangible asset entrusted to the Delta Dental Bellwether Defendants. Plaintiff also faces a substantial and imminent risk of future harm.

5. Michelle Gonsalves

465. Plaintiff Michelle Gonsalves is, and at all times mentioned herein was, an individual citizen of the State of New York, residing in New York, New York.

466. Plaintiff is a current customer of DDNY and was a customer at the time of the Data Breach. Plaintiff receives Delta Dental insurance through her employer.

467. Plaintiff Gonsalves provided her Private Information to Delta Dental Bellwether Defendants as a condition of receiving dental insurance.

468. Plaintiff Gonsalves had the reasonable expectation and understanding that Delta Dental Bellwether Defendants would take—at minimum—industry standard precautions to protect, maintain, and safeguard that highly sensitive information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff would not have entrusted her Private Information to Delta Dental Bellwether Defendants had she known that Delta Dental Bellwether Defendants would not take reasonable steps to safeguard her information.

469. Plaintiff Gonsalves received a letter from "Delta Dental of California and affiliates" (referred to in the Notice Letter as "Company") dated February 9, 2024, concerning the Data Breach. The letter explained that cybercriminals exploited a security vulnerability in the systems of one of Delta Dental of California and affiliates' third-party vendors, Progress. As a result, unauthorized individuals accessed or obtained data stored on the platform, including the Plaintiff's information. The letter further states the following:

> **What Happened?**
>
> Progress Software announced a previously unknown vulnerability within their widely used MOVEit file-transfer software program. This vulnerability led to a global data security incident that is reported to have impacted many organizations, including corporations, government agencies, insurance providers, pension funds, financial institutions, state education systems and more. On June 1, 2023, the Company learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application. Immediately after being alerted of the incident, we launched a thorough investigation and took steps to contain and remediate the incident. We stopped access to the MOVEit software, removed the malicious files, conducted a thorough analysis of the MOVEit database, applied the recommended patches, and reset administrative passwords to the MOVEit system. We also enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity, and ransomware activity. On July 6, 2023, our investigation confirmed that the Company information on the MOVEit platform had been accessed and acquired without authorization between May 27, 2023 and May 30, 2023. At that time, we promptly engaged independent third-party experts in computer forensics, analytics, and data mining to determine what information was impacted and with whom it is associated. This extensive investigation and analysis of the data recently concluded and was a critical component in enabling us to identify specific personal information that was acquired from the MOVEit platform. Upon that determination, we have worked diligently to identify any impacted individuals to provide notification. On November 27, 2023, we determined your personal information was affected. In addition to our own investigation, we have also notified law enforcement of the incident and have been cooperating with them since.
>
> **What Information Was Involved?** Your affected information included date of birth, Social Security number, and health insurance information.

470. Since the Data Breach, including prior to being notified by Delta Dental of California and affiliates that her Private Information had been compromised and in the hands of

cybercriminals, Plaintiff has experienced an increase in the amount of intrusive spam calls, texts, and emails she receives.

471. Plaintiff Gonsalves has also received alerts that her Private Information was found on the dark web since the Data Breach occurred.

472. Upon information and belief, Plaintiff Gonsalves's unencrypted Private Information was viewed by unauthorized persons, as evidenced by the notifications that her information was listed on the dark web, and the fact that Plaintiff has experienced an uptick in phishing emails since the Data Breach, among other harms described.

473. The disclosure of her health insurance information is highly offensive due to the deeply personal nature of health and medical data. This Data Breach has caused her significant anxiety, increased concerns about the loss of privacy, and fears over the potential misuse of her sensitive information by cybercriminals. She now faces a serious risk of identity theft, credit fraud, and other potential harms, both at present and in the future.

474. Plaintiff Gonsalves values her privacy and is very careful about storing and sharing sensitive Private Information. Plaintiff would not have entrusted her Private Information to Delta Dental Bellwether Defendants had she known of their inadequate and lax data security policies and practices.

475. Plaintiff Gonsalves has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Delta Dental of California and affiliates' possession, is protected and safeguarded from future breaches.

476. As a direct and proximate result of the Data Breach, Plaintiff Gonsalves has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her financial accounts to reduce the risk of future identity theft and fraud.

477. To date, as a result of the Data Breach, Plaintiff Gonsalves has spent over fifteen hours researching the details of the Data Breach. Plaintiff has also expended time and effort checking her credit and financial accounts for any unauthorized, suspicious activity, a practice that Plaintiff Gonsalves will need to continue indefinitely to protect against and/or remedy fraud and identity theft.

478. Had Delta Dental of California and affiliates not delayed in notifying Plaintiff about the Data Breach, she could have taken additional precautions earlier on to protect her identity and mitigate the harms of the Data Breach.

479. As a result of the Data Breach, Plaintiff Gonsalves anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She has faced and continues to face a risk of fraud and identity theft that will last for her lifetime.

480. Plaintiff Gonsalves suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

481. Had Plaintiff Gonsalves been informed that Delta Dental Bellwether Defendants had insufficient data security measures to protect her Private Information, she would have taken this into account in deciding whether to enroll in Delta Dental insurance, and, at a minimum, Plaintiff would not have paid as much for dental insurance.

482. Plaintiff Gonsalves relied on Delta Dental Bellwether Defendants' policies and promises to implement sufficient regulatory and industry compliant measures to protect her Private Information and privacy rights.

483. Due to the highly sensitive nature of the stolen information and its unauthorized dissemination, Plaintiff has already suffered harm, including damages and a loss in the value of

her Private Information—an intangible asset entrusted to the Delta Dental Bellwether Defendants. Plaintiff also faces a substantial and imminent risk of future harm.

6. Margaret Kavanagh

484. Plaintiff Margaret Kavanagh is, and at all times mentioned herein was, an individual citizen of the State of New York, residing in Pittsford, New York.

485. Plaintiff is a customer of DDPenn and was a customer at the time of the Data Breach. She receives Delta Dental insurance through her husband's employer.

486. Plaintiff Kavanagh provided her Private Information to Delta Dental Bellwether Defendants as a condition of receiving dental insurance from Delta Dental Bellwether Defendants.

487. Plaintiff Kavanagh had the reasonable expectation and understanding that Delta Dental Bellwether Defendants would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that highly sensitive information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff would not have entrusted her Private Information to Delta Dental Bellwether Defendants had she known that Delta Dental Bellwether Defendants would not take reasonable steps to safeguard her information.

488. Plaintiff Kavanagh received a letter from "Delta Dental of California and affiliates" (referred to in the Notice Letter as "Company") dated February 8, 2024, concerning the Data Breach. The letter explained that cybercriminals exploited a security vulnerability in the systems of one of Delta Dental of California and affiliates' third-party vendors, Progress. As a result, unauthorized individuals accessed or obtained data stored on the platform, including the Plaintiff's information. The letter further states the following:

> **What Happened?**
>
> Progress Software announced a previously unknown vulnerability within their widely used MOVEit file-transfer software program. This vulnerability led to a global data security incident that is reported to have impacted many organizations,

> including corporations, government agencies, insurance providers, pension funds, financial institutions, state education systems and more. On June 1, 2023, the Company learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application. Immediately after being alerted of the incident, we launched a thorough investigation and took steps to contain and remediate the incident. We stopped access to the MOVEit software, removed the malicious files, conducted a thorough analysis of the MOVEit database, applied the recommended patches, and reset administrative passwords to the MOVEit system. We also enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity, and ransomware activity. On July 6, 2023, our investigation confirmed that the Company information on the MOVEit platform had been accessed and acquired without authorization between May 27, 2023 and May 30, 2023. At that time, we promptly engaged independent third-party experts in computer forensics, analytics, and data mining to determine what information was impacted and with whom it is associated. This extensive investigation and analysis of the data recently concluded and was a critical component in enabling us to identify specific personal information that was acquired from the MOVEit platform. Upon that determination, we have worked diligently to identify any impacted individuals to provide notification. On November 27, 2023, we determined your personal information was affected. In addition to our own investigation, we have also notified law enforcement of the incident and have been cooperating with them since.
>
> **What Information Was Involved?** Your affected information included date of birth, Social Security number, and health insurance information**.**

489. Since the Data Breach, Plaintiff Kavanagh discovered fraudulent charges on her debit cards. Specifically, she discovered approximately $165 of unauthorized Chase Bank debit card charges and withdrawals in February and April 2024.

490. Plaintiff has also received alerts that her Private Information was found on the dark web since the Data Breach occurred.

491. As a consequence of the fraudulent activity, her bank needed to issue her a new debit card.

492. Upon information and belief, Plaintiff's unencrypted Private Information was viewed by unauthorized persons, as evidenced by the notifications she received that her information was listed on the dark web since the Data Breach, among other harms described.

493. The disclosure of her health insurance information is highly offensive due to the deeply personal nature of health and medical data. This Data Breach has caused her significant anxiety, increased concerns about the loss of privacy, and fears over the potential misuse of her sensitive information by cybercriminals. She now faces a serious risk of identity theft, credit fraud, and other potential harms, both at present and in the future.

494. Plaintiff Kavanagh values her privacy and is very careful about storing and sharing sensitive Private Information. Plaintiff would not have entrusted her Private Information to Delta Dental Bellwether Defendants had she known of their inadequate and lax data security policies and practices.

495. Plaintiff Kavanagh has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Delta Dental of California and affiliates' possession, is protected and safeguarded from future breaches.

496. As a direct and proximate result of the Data Breach, Plaintiff Kavanagh has made reasonable efforts to mitigate the impact of the Data Breach, including by investigating fraudulent and suspicious activity she experienced, contacting her bank about the fraudulent activity she experienced, expending time to get fraudulent charges reversed, and by regularly and closely monitoring her financial accounts to reduce the risk of future identity theft and fraud.

497. To date, as a result of the Data Breach, Plaintiff has spent several hours researching the details of the Data Breach and performing those tasks to mitigate the harms. Plaintiff has also expended time and effort checking her financial accounts for any unauthorized, suspicious activity, a practice that she will need to continue indefinitely to protect against and/or remedy fraud and identity theft.

498. Had Delta Dental of California and affiliates not delayed in notifying Plaintiff about the Data Breach, she could have taken additional precautions earlier on to protect her identity and mitigate the harms of the Data Breach.

499. As a result of the Data Breach, Plaintiff Kavanagh anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She has faced and continues to face a risk of fraud and identity theft that will last for her lifetime.

500. Plaintiff Kavanagh suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

501. Had Plaintiff Kavanagh been informed that Delta Dental Bellwether Defendants had insufficient data security measures to protect her Private Information, she would have taken this into account in deciding whether to enroll in Delta Dental insurance, and, at a minimum, Plaintiff would not have paid as much for dental insurance.

502. Plaintiff Kavanagh relied on Delta Dental Bellwether Defendants' policies and promises to implement sufficient regulatory and industry compliant measures to protect her Private Information and privacy rights.

503. Due to the highly sensitive nature of the stolen information and its unauthorized dissemination, Plaintiff has already suffered harm, including damages and a loss in the value of her Private Information—an intangible asset entrusted to the Delta Dental Bellwether Defendants. Plaintiff also faces a substantial and imminent risk of future harm.

7. John Meeks

504. Plaintiff John Meeks is, and at all times mentioned herein was, an individual citizen of the Iowa, residing in Cedar Rapids, Iowa.

505. Plaintiff Meeks was a customer of DDIC at the time of the Data Breach.

506. Plaintiff Meeks provided his Private Information to Delta Dental Bellwether Defendants as a condition of receiving dental insurance.

507. Plaintiff Meeks had the reasonable expectation and understanding that Delta Dental Bellwether Defendants would take—at minimum—industry standard precautions to protect, maintain, and safeguard that highly sensitive information from unauthorized users or disclosure, and would timely notify him of any data security incidents. Plaintiff would not have entrusted his Private Information to Delta Dental Bellwether Defendants had he known that Delta Dental Bellwether Defendants would not take reasonable steps to safeguard his Private Information.

508. Plaintiff Meeks received a letter from "Delta Dental of California and affiliates" (referred to in the Notice Letter as "Company") dated December 15, 2023, concerning the Data Breach. The letter explained that cybercriminals exploited a security vulnerability in the systems of one of Delta Dental of California and affiliates' third-party vendors, Progress. As a result, unauthorized individuals accessed or obtained data stored on the platform, including Plaintiff's information. The letter further states the following:

> **What Happened?**
>
> Progress Software announced a previously unknown vulnerability within their widely used MOVEit file-transfer software program. This vulnerability led to a global data security incident that is reported to have impacted many organizations, including corporations, government agencies, insurance providers, pension funds, financial institutions, state education systems and more. On June 1, 2023, the Company learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application. Immediately after being alerted of the incident, we launched a thorough investigation and took steps to contain and remediate the incident. We stopped access to the MOVEit software, removed the malicious files, conducted a thorough analysis of the MOVEit database, applied the recommended patches, and reset administrative passwords to the MOVEit system. We also enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity, and ransomware activity. On July 6, 2023, our investigation confirmed that the Company information on the MOVEit platform had been accessed and acquired without authorization between May 27, 2023 and May 30, 2023. At that time, we promptly engaged independent third-party experts in computer forensics, analytics, and data mining to determine what

> information was impacted and with whom it is associated. This extensive investigation and analysis of the data recently concluded and was a critical component in enabling us to identify specific personal information that was acquired from the MOVEit platform. Upon that determination, we have worked diligently to identify any impacted individuals to provide notification. On November 27, 2023, we determined your personal information was affected. In addition to our own investigation, we have also notified law enforcement of the incident and have been cooperating with them since.
>
> **What Information Was Involved?** Your affected information included date of birth, Social Security number, provider name, health insurance information, and treatment cost information.

509. Since the Data Breach, Plaintiff Meeks has experienced fraudulent, unauthorized activity from another country on his Greenstate Credit Union cards. The bank cancelled and reissued his card after each fraudulent charge.

510. Plaintiff has also received alerts that his Private Information was found on the dark web since the Data Breach occurred.

511. Upon information and belief, Plaintiff's unencrypted Private Information was viewed by unauthorized persons, as evidenced by the fact that Plaintiff received notifications that his information was listed on the dark web and that he has experienced fraudulent activity in his accounts since the Data Breach.

512. The disclosure of his health insurance information is highly offensive due to the deeply personal nature of health and medical data. This Data Breach has caused him significant anxiety, increased concerns about the loss of privacy, and fears over the potential misuse of his sensitive information by cybercriminals. He now faces a serious risk of identity theft, credit fraud, and other potential harms, both at present and in the future.

513. Plaintiff Meeks values his privacy and is very careful about storing and sharing sensitive Private Information. Plaintiff would not have entrusted his Private Information to Delta

Dental Bellwether Defendants had he known of their inadequate and lax data security policies and practices.

514. Plaintiff Meeks has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Delta Dental of California and affiliates' possession, is protected and safeguarded from future breaches.

515. As a direct and proximate result of the Data Breach, Plaintiff Meeks has made reasonable efforts to mitigate the impact of the Data Breach, including by investigating fraudulent and suspicious activity he experienced, contacting his bank, and regularly and closely monitoring his financial accounts to reduce the risk of future identity theft and fraud. He had to cancel his credit cards for three consecutive months, and the bank reissued him new ones.

516. As a result of the Data Breach, Plaintiff has obtained the credit monitoring service Experian.

517. To date, as a result of the Data Breach, Plaintiff Meeks has spent over 40 hours monitoring and investigating fraudulent and suspicious activity, as well as contacting his banks to resolve the unauthorized charges, and checking his credit and financial accounts for any unauthorized and suspicious activity, a practice that Plaintiff Meeks will need to continue indefinitely to protect against and/or remedy fraud and identity theft.

518. Had Delta Dental of California and affiliates not delayed in notifying him about the Data Breach, he could have taken precautions earlier on to protect his identity and mitigate the harms of the Data Breach.

519. As a result of the Data Breach, Plaintiff Meeks anticipates spending considerable money and additional time on an ongoing basis to try to mitigate and address the harms caused by

the Data Breach. He has faced and continues to face a risk of fraud and identity theft that will last for his lifetime.

520. Plaintiff Meeks suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

521. Had Plaintiff Meeks been informed that Delta Dental Bellwether Defendants had insufficient data security measures to protect his Private Information, he would have taken this into account in deciding whether to enroll in Delta Dental insurance, and, at a minimum, Plaintiff would not have paid as much for dental insurance.

522. Plaintiff Meeks relied on Delta Dental Bellwether Defendants' policies and promises to implement sufficient regulatory and industry compliant measures to protect his Private Information and privacy rights.

523. Due to the highly sensitive nature of the stolen information and its unauthorized dissemination, Plaintiff has already suffered harm, including damages and a loss in the value of his Private Information—an intangible asset entrusted to the Delta Dental Bellwether Defendants. Plaintiff also faces a substantial and imminent risk of future harm.

8. Terrill Mendler

524. Plaintiff Terrill Mendler is, and at all times mentioned herein was, an individual citizen of the State of Florida, residing in Jacksonville, Florida.

525. Plaintiff was a customer of DDIC at the time of the Data Breach and received dental insurance through her employer. Plaintiff is now retired and is now a customer of Delta Dental Bellwether Defendants through an independent plan.

526. Plaintiff Mendler provided her Private Information to Delta Dental Bellwether Defendants as a condition of receiving dental insurance.

527. Plaintiff Mendler had the reasonable expectation and understanding that Delta Dental Bellwether Defendants would take—at minimum—industry standard precautions to protect, maintain, and safeguard that highly sensitive information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff would not have entrusted her Private Information to Delta Dental Bellwether Defendants had she known that Delta Dental Bellwether Defendants would not take reasonable steps to safeguard her information.

528. Plaintiff Mendler received a letter from "Delta Dental of California and affiliates" (referred to in the Notice Letter as "Company") dated January 12, 2024 concerning the Data Breach. The letter stated that cybercriminals exploited a security vulnerability within the systems of one of Delta Dental of California and affiliates' third-party vendors, Progress. As a result, unauthorized individuals accessed or obtained data stored on the platform, including the Plaintiff's information. The letter further states the following:

> **What Happened?**
>
> Progress Software announced a previously unknown vulnerability within their widely used MOVEit file-transfer software program. This vulnerability led to a global data security incident that is reported to have impacted many organizations, including corporations, government agencies, insurance providers, pension funds, financial institutions, state education systems and more. On June 1, 2023, the Company learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application. Immediately after being alerted of the incident, we launched a thorough investigation and took steps to contain and remediate the incident. We stopped access to the MOVEit software, removed the malicious files, conducted a thorough analysis of the MOVEit database, applied the recommended patches, and reset administrative passwords to the MOVEit system. We also enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity, and ransomware activity. On July 6, 2023, our investigation confirmed that the Company information on the MOVEit platform had been accessed and acquired without authorization between May 27, 2023 and May 30, 2023. At that time, we promptly engaged independent third-party experts in computer forensics, analytics, and data mining to determine what information was impacted and with whom it is associated. This extensive investigation and analysis of the data recently concluded and was a critical component in enabling us to identify specific personal information that was acquired from the MOVEit platform. Upon that determination, we have worked

> diligently to identify any impacted individuals to provide notification. On November 27, 2023, we determined your personal information was affected. In addition to our own investigation, we have also notified law enforcement of the incident and have been cooperating with them since.
>
> **What Information Was Involved?** Your affected information included date of birth, Social Security number, and health insurance information.

529. Since the Data Breach, including prior to being notified by Delta Dental of California and affiliates that her Private Information had been compromised and in the hands of cybercriminals, Plaintiff has experienced an increase in the amount of intrusive spam calls, texts, and emails she receives.

530. Since the Data Breach, Plaintiff Mendler discovered fraudulent charges on her bank cards. For example, an unauthorized user purchased a ticket for a cruise ship, which her credit card provider denied, as well as at least one smaller purchase, which was approved. As a consequence of the fraudulent activity, her bank needed to issue her a new account number.

531. Upon information and belief, Plaintiff Mendler's unencrypted Private Information was viewed by unauthorized persons, as evidenced by the fact that Plaintiff has experienced an uptick in phishing emails since the Data Breach, among other harms.

532. The disclosure of her health insurance information is highly offensive due to the intensely personal nature of one's personal health and medical related information. The Data Breach has caused her significant anxiety, increased concerns about the loss of her privacy, and fears over the potential misuse of her highly sensitive Private Information by cybercriminals. She now faces a serious risk of identity theft, credit fraud, and other potential harms, both at present and in the future.

533. Plaintiff Mendler values her privacy and is very careful about storing and sharing sensitive Private Information. Plaintiff would not have entrusted her Private Information to Delta

Dental Bellwether Defendants had she known of their inadequate and lax data security policies and practices.

534. Plaintiff Mendler has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Delta Dental of California and affiliates' possession, is protected and safeguarded from future breaches.

535. As a direct and proximate result of the Data Breach, Plaintiff Mendler has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her financial accounts for unauthorized, suspicious activity to reduce the risk of future identity theft and fraud, as well as contacting her bank to reverse the fraudulent charges.

536. As a result of the Data Breach, Plaintiff has obtained the credit monitoring service, Kroll, offered for a two-year period by Delta Dental of California and affiliates.

537. To date, as a result of the Data Breach, Plaintiff Mendler has spent several hours researching the details of the Data Breach. Plaintiff has also expended time and effort reversing the fraudulent charges and checking her credit and financial accounts for any unauthorized, suspicious activity, a practice that Plaintiff Mendler will need to continue indefinitely to protect against and/or remedy fraud and identity theft.

538. Had Delta Dental of California and affiliates not delayed in notifying Plaintiff about the Data Breach, she could have taken additional precautions earlier on to protect her identity and mitigate the harms of the Data Breach.

539. As a result of the Data Breach, Plaintiff Mendler anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She has faced and continues to face a risk of fraud and identity theft that will last for her lifetime.

540. Plaintiff Mendler suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

541. Had Plaintiff Mendler been informed that Delta Dental Bellwether Defendants had insufficient data security measures to protect her Private Information, she would have taken this into account in deciding whether to enroll in Delta Dental insurance, and, at a minimum, Plaintiff would not have paid as much for dental insurance.

542. Plaintiff Mendler relied on Delta Dental Bellwether Defendants' policies and promises to implement sufficient regulatory and industry compliant measures to protect her Private Information and privacy rights.

543. Given the highly sensitive nature of the information stolen, and its subsequent dissemination to unauthorized parties, Plaintiff has already suffered injury in the form of damages and diminution in the value of her Private Information— a form of intangible property that Plaintiff entrusted to Delta Dental Bellwether Defendants. Plaintiff remains at a substantial and imminent risk of future harm.

9. Manuel Mendoza

544. Plaintiff Manuel Mendoza is, and at all times mentioned herein was, an individual citizen of the State of Texas, residing in LaPorte, Texas.

545. Plaintiff is the spouse of policyholder and customer of DDIC, Emma Mendoza. Plaintiff was a customer of Delta Dental at the time of the Data Breach. They both receive Delta Dental insurance through his wife's employer.

546. Plaintiff Mendoza's Texas Dental Choice PPO Plan is provided DDIC.

547. Plaintiff Mendoza provided his Private Information to Delta Dental Bellwether Defendants as a condition of receiving dental insurance through his wife's Delta Dental insurance plan.

548. Plaintiff Mendoza had the reasonable expectation and understanding that Delta Dental Bellwether Defendants would take—at minimum—industry standard precautions to protect, maintain, and safeguard that highly sensitive information from unauthorized users or disclosure, and would timely notify him of any data security incidents. Plaintiff would not have entrusted his Private Information to Delta Dental Bellwether Defendants had he known that Delta Dental Bellwether Defendants would not take reasonable steps to safeguard his information.

549. Plaintiff Mendoza received a letter from "Delta Dental of California and affiliates" (referred to in the Notice Letter as "Company") dated January 29, 2024 concerning the Data Breach. The letter explained that cybercriminals exploited a security vulnerability in the systems of one of Delta Dental of California and affiliates' third-party vendors, Progress. As a result, unauthorized individuals accessed or obtained data stored on the platform, including the Plaintiff's information. The letter further states the following:

> **What Happened?**
>
> Progress Software announced a previously unknown vulnerability within their widely used MOVEit file-transfer software program. This vulnerability led to a global data security incident that is reported to have impacted many organizations, including corporations, government agencies, insurance providers, pension funds, financial institutions, state education systems and more. On June 1, 2023, the Company learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application. Immediately after being alerted of the incident, we launched a thorough investigation and took steps to contain and remediate the incident. We stopped access to the MOVEit software, removed the malicious files, conducted a thorough analysis of the MOVEit database, applied the recommended patches, and reset administrative passwords to the MOVEit system. We also enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity, and ransomware activity. On July 6, 2023, our investigation confirmed that the Company information on the MOVEit platform had been accessed and acquired without authorization between May 27, 2023 and May 30, 2023. At that time, we promptly engaged independent third-party experts in computer forensics, analytics, and data mining to determine what information was impacted and with whom it is associated. This extensive investigation and analysis of the data recently concluded and was a critical component in enabling us to identify specific personal information that was acquired from the MOVEit platform. Upon that determination, we have worked

> diligently to identify any impacted individuals to provide notification. On November 27, 2023, we determined your personal information was affected. In addition to our own investigation, we have also notified law enforcement of the incident and have been cooperating with them since.
>
> **What Information Was Involved?** Your affected information included date of birth and health insurance information**.**

550. Since the Data Breach, including prior to being notified by Delta Dental of California and affiliates that his Private Information had been compromised and in the hands of cybercriminals, Plaintiff has discovered fraudulent charges on his and his wife's Welby Financial debit and credit cards. Plaintiff had to cancel the cards after each charge and have hem reissued.

551. Upon information and belief, Plaintiff Mendoza's unencrypted Private Information was viewed by unauthorized persons, as evidenced by the fact that Plaintiff has discovered fraudulent charges on his bank cards.

552. The disclosure of his health insurance information is highly offensive due to the deeply personal nature of health and medical data. This Data Breach has caused him significant anxiety, increased concerns about the loss of privacy, and fears over the potential misuse of his sensitive information by cybercriminals. He now faces a serious risk of identity theft, credit fraud, and other potential harms, both at present and in the future.

553. Plaintiff Mendoza values his privacy and is very careful about storing and sharing sensitive Private Information. Plaintiff would not have entrusted his Private Information to Delta Dental Bellwether Defendants had he known of their inadequate and lax data security policies and practices.

554. Plaintiff Mendoza has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Delta Dental of California and affiliates' possession, is protected and safeguarded from future breaches.

555. As a direct and proximate result of the Data Breach, Plaintiff Mendoza has made reasonable efforts to mitigate the impact of the Data Breach, including by investigating fraudulent and suspicious activity he experienced, contacting banks, credit card companies, or other vendors about the suspicious, fraudulent activity he experienced, expending time to get fraudulent charges reversed, and by regularly and closely monitoring his financial accounts to reduce the risk of future identity theft and fraud.

556. To date, as a result of the Data Breach, Plaintiff Mendoza has spent several hours researching the details of the Data Breach and performing those mitigation tasks. Plaintiff has also expended time and effort checking his credit and financial accounts for any unauthorized, suspicious activity, a practice that Plaintiff Mendoza will need to continue indefinitely to protect against and/or remedy fraud and identity theft.

557. Had Delta Dental of California and affiliates not delayed in notifying Plaintiff about the Data Breach, he could have taken additional precautions earlier on to protect his identity and mitigate the harms of the Data Breach.

558. As a result of the Data Breach, Plaintiff Mendoza anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. He has faced and continues to face a risk of fraud and identity theft that will last for his lifetime.

559. Plaintiff Mendoza suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

560. Had Plaintiff Mendoza been informed that Delta Dental Bellwether Defendants had insufficient data security measures to protect his Private Information, he would have taken this

into account in deciding whether to enroll in Delta Dental insurance, and, at a minimum, Plaintiff would not have paid as much for dental insurance.

561. Plaintiff Mendoza relied on Delta Dental Bellwether Defendants' policies and promises to implement sufficient regulatory and industry compliant measures to protect his Private Information and privacy rights.

562. Due to the highly sensitive nature of the stolen information and its unauthorized dissemination, Plaintiff has already suffered harm, including damages and a loss in the value of his Private Information—an intangible asset entrusted to the Delta Dental Bellwether Defendants. Plaintiff also faces a substantial and imminent risk of future harm.

10. Ricardo Moralez

563. Plaintiff Ricardo Moralez is, and at all times mentioned herein was, an individual citizen of the State of California, residing in Montclair, California.

564. Plaintiff Moralez is a current customer of DDCA and was a customer at the time of the Data Breach. Plaintiff receives Delta Dental insurance through the state of California's health insurance marketplace.

565. Plaintiff Moralez provided his Private Information to Delta Dental Bellwether Defendants as a condition of receiving dental insurance.

566. Plaintiff Moralez had the reasonable expectation and understanding that Delta Dental Bellwether Defendants would take—at minimum—industry standard precautions to protect, maintain, and safeguard that highly sensitive information from unauthorized users or disclosure, and would timely notify him of any data security incidents. Plaintiff would not have entrusted his Private Information to Delta Dental Bellwether Defendants had he known that Delta Dental Bellwether Defendants would not take reasonable steps to safeguard his information.

567. Plaintiff Moralez received a letter from "Delta Dental of California and affiliates" (referred to in the Notice Letter as "Company") dated January 12, 2024 concerning the Data Breach. The letter explained that cybercriminals exploited a security vulnerability in the systems of one of Delta Dental of California and affiliates' third-party vendors, Progress. As a result, unauthorized individuals accessed or obtained data stored on the platform, including the Plaintiff's information. The letter further states the following:

> **What Happened?**
>
> Progress Software announced a previously unknown vulnerability within their widely used MOVEit file-transfer software program. This vulnerability led to a global data security incident that is reported to have impacted many organizations, including corporations, government agencies, insurance providers, pension funds, financial institutions, state education systems and more. On June 1, 2023, the Company learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application. Immediately after being alerted of the incident, we launched a thorough investigation and took steps to contain and remediate the incident. We stopped access to the MOVEit software, removed the malicious files, conducted a thorough analysis of the MOVEit database, applied the recommended patches, and reset administrative passwords to the MOVEit system. We also enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity, and ransomware activity. On July 6, 2023, our investigation confirmed that the Company information on the MOVEit platform had been accessed and acquired without authorization between May 27, 2023 and May 30, 2023. At that time, we promptly engaged independent third-party experts in computer forensics, analytics, and data mining to determine what information was impacted and with whom it is associated. This extensive investigation and analysis of the data recently concluded and was a critical component in enabling us to identify specific personal information that was acquired from the MOVEit platform. Upon that determination, we have worked diligently to identify any impacted individuals to provide notification. On November 27, 2023, we determined your personal information was affected. In addition to our own investigation, we have also notified law enforcement of the incident and have been cooperating with them since.
>
> **What Information Was Involved?** Your affected information included date of birth, Social Security number, and health insurance information.

568. Since the Data Breach, including prior to being notified by Delta Dental of California and affiliates that his Private Information had been compromised and in the hands of

cybercriminals, Plaintiff has experienced an increase in the amount of intrusive spam calls, texts, and emails he receives.

569. Since the Data Breach, new accounts, loans, or lines of credit were opened in Plaintiff Moralez's name. He received emails alleging that he took loans from Speedy Cash and American Advance, however, Plaintiff Moralez never took out said loans.

570. Upon information and belief, Plaintiff's unencrypted Private Information was viewed by unauthorized persons, as evidenced by the received the fact that Plaintiff has experienced an uptick in phishing emails since the Data Breach and that loans were taken out in his name, among other harms described.

571. The disclosure of his health insurance information is highly offensive due to the deeply personal nature of health and medical data. This Data Breach has caused him significant anxiety, increased concerns about the loss of privacy, and fears over the potential misuse of his sensitive information by cybercriminals. He now faces a serious risk of identity theft, credit fraud, and other potential harms, both at present and in the future.

572. Plaintiff Moralez values his privacy and is very careful about storing and sharing sensitive Private Information. Plaintiff would not have entrusted his Private Information to Delta Dental Bellwether Defendants had he known of their inadequate and lax data security policies and practices.

573. Plaintiff Moralez has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Delta Dental of California and affiliates' possession, is protected and safeguarded from future breaches.

574. As a direct and proximate result of the Data Breach, Plaintiff Moralez has made reasonable efforts to mitigate the impact of the Data Breach, including by contacting banks, credit

card companies, or other vendors about suspicious, fraudulent activity he experienced, as well as by regularly and closely monitoring his financial accounts for any unauthorized, suspicious activity, to reduce the risk of future identity theft and fraud.

575. To date, as a result of the Data Breach, Plaintiff Moralez has expended several hours researching the details of the Data Breach as well as great time and effort trying to mitigate the harms of the Data Breach, as described, which are practices that Plaintiff Moralez will need to continue indefinitely to protect against and/or remedy fraud and identity theft.

576. Had Delta Dental of California and affiliates not delayed in notifying Plaintiff about the Data Breach, he could have taken additional precautions earlier on to protect his identity and mitigate the harms of the Data Breach.

577. As a result of the Data Breach, Plaintiff Moralez anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. He has faced and continues to face a risk of fraud and identity theft that will last for his lifetime.

578. Plaintiff Moralez suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

579. Had Plaintiff Moralez been informed that Delta Dental Bellwether Defendants had insufficient data security measures to protect his Private Information, he would have taken this into account in deciding whether to enroll in Delta Dental insurance, and, at a minimum, Plaintiff would not have paid as much for dental insurance.

580. Plaintiff Moralez relied on Delta Dental Bellwether Defendants' policies and promises to implement sufficient regulatory and industry compliant measures to protect his Private Information and privacy rights.

581. Due to the highly sensitive nature of the stolen information and its unauthorized dissemination, Plaintiff has already suffered harm, including damages and a loss in the value of his Private Information—an intangible asset entrusted to the Delta Dental Bellwether Defendants. Plaintiff also faces a substantial and imminent risk of future harm.

11. Hannah Polikowsky

582. Plaintiff Hannah Polikowsky is, and at all times mentioned herein was, an individual citizen of the State of Tennessee, residing in Memphis, Tennessee.

583. Plaintiff is a current customer of DDCA and was a customer at the time of the Data Breach. Plaintiff receives Delta Dental insurance through her employer.

584. Plaintiff Polikowsky provided her Private Information to Delta Dental Bellwether Defendants as a condition of receiving dental insurance.

585. Plaintiff Polikowsky had the reasonable expectation and understanding that Delta Dental Bellwether Defendants would take—at minimum—industry standard precautions to protect, maintain, and safeguard that highly sensitive information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff would not have entrusted her Private Information to Delta Dental had she known that Delta Dental would not take reasonable steps to safeguard her information.

586. Plaintiff Polikowsky received a letter from "Delta Dental of California and affiliates" (referred to in the Notice Letter as "Company") dated February 9, 2024 concerning the Data Breach. The letter explained that cybercriminals exploited a security vulnerability in the systems of one of Delta Dental of California and affiliates' third-party vendors, Progress. As a result, unauthorized individuals accessed or obtained data stored on the platform, including the Plaintiff's information. The letter further states the following:

What Happened?

Progress Software announced a previously unknown vulnerability within their widely used MOVEit file-transfer software program. This vulnerability led to a global data security incident that is reported to have impacted many organizations, including corporations, government agencies, insurance providers, pension funds, financial institutions, state education systems and more. On June 1, 2023, the Company learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application. Immediately after being alerted of the incident, we launched a thorough investigation and took steps to contain and remediate the incident. We stopped access to the MOVEit software, removed the malicious files, conducted a thorough analysis of the MOVEit database, applied the recommended patches, and reset administrative passwords to the MOVEit system. We also enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity, and ransomware activity. On July 6, 2023, our investigation confirmed that the Company information on the MOVEit platform had been accessed and acquired without authorization between May 27, 2023 and May 30, 2023. At that time, we promptly engaged independent third-party experts in computer forensics, analytics, and data mining to determine what information was impacted and with whom it is associated. This extensive investigation and analysis of the data recently concluded and was a critical component in enabling us to identify specific personal information that was acquired from the MOVEit platform. Upon that determination, we have worked diligently to identify any impacted individuals to provide notification. On November 27, 2023, we determined your personal information was affected. In addition to our own investigation, we have also notified law enforcement of the incident and have been cooperating with them since.

What Information Was Involved? Your affected information included date of birth, Social Security number, and health insurance information**.**

587. Since the Data Breach, including prior to being notified by Delta Dental of California and affiliates that her Private Information had been compromised and in the hands of cybercriminals, Plaintiff Polikowsky has experienced an increase in the amount of intrusive spam calls, texts, and emails she receives.

588. Since the Data Breach, Plaintiff Polikowsky discovered fraudulent charges on her bank card. Specifically, in or around January 2024, she discovered an unauthorized purchase for approximately $1,100. She and her husband investigated the fraudulent activity and confirmed the unauthorized purchaser had obtained her credit card information and sent the products to an

unknown address in Georgia. Plaintiff was required to dispute the charge with her bank to get the charges reversed and obtain a new credit card.

589. Upon information and belief, Plaintiff's unencrypted Private Information was viewed by unauthorized persons, as evidenced by the received the fact that Plaintiff has experienced fraudulent activity on her credit card since and an uptick in phishing emails since the Data Breach, among other harms.

590. The disclosure of her health insurance information is highly offensive due to the deeply personal nature of health and medical data. This Data Breach has caused her significant anxiety, increased concerns about the loss of privacy, and fears over the potential misuse of her sensitive information by cybercriminals. She now faces a serious risk of identity theft, credit fraud, and other potential harms, both at present and in the future.

591. Plaintiff Polikowsky values her privacy and is very careful about storing and sharing sensitive Private Information. Plaintiff would not have entrusted her Private Information to Delta Dental Bellwether Defendants had she known of their inadequate and lax data security policies and practices.

592. Plaintiff Polikowsky has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Delta Dental of California and affiliates' possession, is protected and safeguarded from future breaches.

593. As a direct and proximate result of the Data Breach, Plaintiff Polikowsky has made reasonable efforts to mitigate the impact of the Data Breach, including by investigating fraudulent and suspicious activity she experienced, contacting banks, credit card companies, or other vendors about the suspicious, fraudulent activity she experienced, expending time to get fraudulent charges

reversed, and by regularly and closely monitoring her financial accounts to reduce the risk of future identity theft and fraud.

594. As a result of the Data Breach, Plaintiff has obtained the credit monitoring service, Kroll, offered for a two-year period by Delta Dental of California and affiliates. Plaintiff also froze her credit at the beginning of May 2024 at all three credit bureaus (Equifax, Experian, and TransUnion). Plaintiff could not freeze her credit until her home sale closure on April 5, 2024, a purchase necessitating credit review. After said purchase, Plaintiff also signed up for Fraud Alert with the Shelby County Register of Deeds to mitigate the risk of anyone filing a fraudulent deed on her home.

595. To date, as a result of the Data Breach, Plaintiff Polikowsky has expended over twenty-five hours between researching the details of the Data Breach and her efforts trying to mitigate the harms of the Data Breach, as described. Plaintiff will need to indefinitely continue to monitor her credit and financial accounts for any unauthorized, suspicious activity and expend time, energy, and effort to protect against and/or remedy fraud and identity theft.

596. Had Delta Dental of California and affiliates not delayed in notifying Plaintiff Polikowsky about the Data Breach, she could have taken additional precautions earlier on to protect her identity and mitigate the harms of the Data Breach.

597. As a result of the Data Breach, Plaintiff Polikowsky anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She has faced and continues to face a risk of fraud and identity theft that will last for her lifetime.

598. Plaintiff Polikowsky suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach.

599. Had Plaintiff Polikowsky been informed that Delta Dental Bellwether Defendants had insufficient data security measures to protect her Private Information, she would have taken this into account in deciding whether to enroll in Delta Dental insurance, and, at a minimum, Plaintiff would not have paid as much for dental insurance.

600. Plaintiff Polikowsky relied on Delta Dental Bellwether Defendants' policies and promises to implement sufficient regulatory and industry compliant measures to protect her Private Information and privacy rights.

601. Due to the highly sensitive nature of the stolen information and its unauthorized dissemination, Plaintiff has already suffered harm, including damages and a loss in the value of her Private Information—an intangible asset entrusted to the Delta Dental Bellwether Defendants. Plaintiff also faces a substantial and imminent risk of future harm.

12. Diamond Roberts

602. Plaintiff Diamond Roberts is, and at all times mentioned herein was, an individual citizen of the State of Texas residing in Manvel, Texas.

603. Plaintiff Roberts is a current customer of DDPenn and was a customer at the time of the Data Breach. She receives Delta Dental insurance through her employer.

604. Plaintiff Roberts provided substantial amounts of her Private Information to Delta Dental Bellwether Defendants as a condition of receiving dental insurance.

605. Plaintiff Roberts had the reasonable expectation and understanding that Delta Dental Bellwether Defendants would take—at minimum—industry standard precautions to protect, maintain, and safeguard that highly sensitive information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff would not have entrusted her Private Information to Delta Dental Bellwether Defendants had she known that Delta Dental Bellwether Defendants would not take reasonable steps to safeguard it.

606. Plaintiff Roberts received a letter from "Delta Dental of California and affiliates" (referred to in the Notice Letter as "Company") dated January 19, 2024, concerning the Data Breach. The letter explained that cybercriminals exploited a security vulnerability in the systems of one of Delta Dental of California and affiliates' third-party vendors, Progress. As a result, unauthorized individuals accessed or obtained data stored on the platform, including the Plaintiff's information. The letter further states the following:

> **What Happened?**
>
> Progress Software announced a previously unknown vulnerability within their widely used MOVEit file-transfer software program. This vulnerability led to a global data security incident that is reported to have impacted many organizations, including corporations, government agencies, insurance providers, pension funds, financial institutions, state education systems and more. On June 1, 2023, the Company learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application. Immediately after being alerted of the incident, we launched a thorough investigation and took steps to contain and remediate the incident. We stopped access to the MOVEit software, removed the malicious files, conducted a thorough analysis of the MOVEit database, applied the recommended patches, and reset administrative passwords to the MOVEit system. We also enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity, and ransomware activity. On July 6, 2023, our investigation confirmed that the Company information on the MOVEit platform had been accessed and acquired without authorization between May 27, 2023 and May 30, 2023. At that time, we promptly engaged independent third-party experts in computer forensics, analytics, and data mining to determine what information was impacted and with whom it is associated. This extensive investigation and analysis of the data recently concluded and was a critical component in enabling us to identify specific personal information that was acquired from the MOVEit platform. Upon that determination, we have worked diligently to identify any impacted individuals to provide notification. On November 27, 2023, we determined your personal information was affected. In addition to our own investigation, we have also notified law enforcement of the incident and have been cooperating with them since.
>
> **What Information Was Involved?** Your affected information included date of birth, Social Security number, and health insurance information.

607. Since the Data Breach, she has had to put a credit freeze on her account.

608. Plaintiff Roberts has received alerts that her Private Information was found on the dark web since the Data Breach occurred.

609. As a consequence of the fraudulent activity subsequent to the Breach, Plaintiff Roberts incurred $40 in costs to sign up for a credit report service.

610. Upon information and belief, Plaintiff Robert's unencrypted Private Information was viewed by unauthorized persons, as evidenced by the fact that Plaintiff received notifications that her information was listed on the dark web and that she has experienced an uptick in phishing emails since the Data Breach.

611. The disclosure of her health insurance information is highly offensive due to the deeply personal nature of health and medical data. This Data Breach has caused her significant anxiety, increased concerns about the loss of privacy, and fears over the potential misuse of her sensitive information by cybercriminals. She now faces a serious risk of identity theft, credit fraud, and other potential harms, both at present and in the future.

612. Plaintiff values her privacy and is very careful about storing and sharing sensitive Private Information. Plaintiff would not have entrusted her Private Information to Delta Dental Bellwether Defendants had she known of their inadequate and lax data security policies and practices.

613. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Delta Dental of California and affiliates' possession, is protected and safeguarded from future breaches.

614. As a direct and proximate result of the Data Breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her financial accounts and credit to reduce the risk of future identity theft and fraud.

615. To date, as a result of the Data Breach, Plaintiff has spent several hours researching the details and checking her credit and financial accounts for any unauthorized and suspicious activity, a practice that Plaintiff will need to continue indefinitely to protect against and/or remedy fraud and identity theft.

616. Had Delta Dental of California and affiliates not delayed in notifying her about the Data Breach, she could have taken precautions earlier on to protect her identity and mitigate the harms of the Data Breach.

617. As a result of the Data Breach, Plaintiff anticipates spending considerable money and additional time on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She faced and continues to a face risk of fraud and identity theft presently that will last for her lifetime.

618. Plaintiff suffered lost time, annoyance, interference, inconvenience, and incurred expenses as a result of the Data Breach.

619. Had Plaintiff been informed that Delta Dental Bellwether Defendants had insufficient data security measures to protect her Private Information, she would have taken this into account in deciding whether to enroll in Delta Dental insurance, and, at a minimum, Plaintiff would not have paid as much for dental insurance.

620. Plaintiff relied on Delta Dental Bellwether Defendants' policies and promises to implement sufficient regulatory and industry compliant measures to protect her Private Information and privacy rights.

621. Due to the highly sensitive nature of the stolen information and its unauthorized dissemination, Plaintiff has already suffered harm, including damages and a loss in the value of

her Private Information—an intangible asset entrusted to the Delta Dental Bellwether Defendants. Plaintiff also faces a substantial and imminent risk of future harm.

13. Taneisha Robertson

622. Plaintiff Taneisha Robertson is, and at all times mentioned herein was, an individual citizen of the State of Georgia residing in Douglasville, Georgia.

623. Plaintiff Robertson is a current customer of DDPenn and was a customer at the time of the Data Breach. She receives Delta Dental insurance through her husband's employer.

624. Plaintiff Robertson provided substantial amounts of her and her minor children's Private Information to Delta Dental Bellwether Defendants as a condition of receiving dental insurance.

625. Plaintiff Robertson had the reasonable expectation and understanding that Delta Dental Bellwether Defendants would take—at minimum—industry standard precautions to protect, maintain, and safeguard that highly sensitive information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff would not have entrusted her Private Information to Delta Dental Bellwether Defendants had she known that Delta Dental Bellwether Defendants would not take reasonable steps to safeguard it.

626. Plaintiff Robertson received a letter from "Delta Dental of California and affiliates" (referred to in the Notice Letter as "Company") dated December 15, 2023, concerning the Data Breach.24 The letter explained that cybercriminals exploited a security vulnerability in the systems of one of Delta Dental of California and affiliates' third-party vendors, Progress. As a result,

[24] Plaintiff Robertson's two minor children, Jaylah Robertson and Xion Robertson, also received Data Breach notices from Delta Dental of California and affiliates dated December 15, 2023.

unauthorized individuals accessed or obtained data stored on the platform, including the Plaintiff's information. The letter further states the following:

> **What Happened?**
>
> Progress Software announced a previously unknown vulnerability within their widely used MOVEit file-transfer software program. This vulnerability led to a global data security incident that is reported to have impacted many organizations, including corporations, government agencies, insurance providers, pension funds, financial institutions, state education systems and more. On June 1, 2023, the Company learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application. Immediately after being alerted of the incident, we launched a thorough investigation and took steps to contain and remediate the incident. We stopped access to the MOVEit software, removed the malicious files, conducted a thorough analysis of the MOVEit database, applied the recommended patches, and reset administrative passwords to the MOVEit system. We also enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity, and ransomware activity. On July 6, 2023, our investigation confirmed that the Company information on the MOVEit platform had been accessed and acquired without authorization between May 27, 2023 and May 30, 2023. At that time, we promptly engaged independent third-party experts in computer forensics, analytics, and data mining to determine what information was impacted and with whom it is associated. This extensive investigation and analysis of the data recently concluded and was a critical component in enabling us to identify specific personal information that was acquired from the MOVEit platform. Upon that determination, we have worked diligently to identify any impacted individuals to provide notification. On November 27, 2023, we determined your personal information was affected. In addition to our own investigation, we have also notified law enforcement of the incident and have been cooperating with them since.
>
> **What Information Was Involved?** Your affected information included date of birth, Social Security number, provider name, health insurance information, and treatment cost information.

627. Since the Data Breach, she has had to put a credit freeze on her account.

628. Plaintiff Robertson has received alerts that her Private Information was found on the dark web since the Data Breach occurred.

629. As a consequence of the fraudulent activity subsequent to the Breach, Plaintiff Robertson incurred $40 in costs to sign up for a credit report service.

630. Upon information and belief, Plaintiff Robertson's unencrypted Private Information was viewed by unauthorized persons, as evidenced by the fact that Plaintiff received notifications that her information was listed on the dark web and that she has experienced an uptick in phishing emails since the Data Breach.

631. The disclosure of her health insurance information is highly offensive due to the deeply personal nature of health and medical data. This Data Breach has caused her significant anxiety, increased concerns about the loss of privacy, and fears over the potential misuse of her sensitive information by cybercriminals. She now faces a serious risk of identity theft, credit fraud, and other potential harms, both at present and in the future.

632. Plaintiff Robertson values her privacy and is very careful about storing and sharing sensitive Private Information. Plaintiff would not have entrusted her or her children's Private Information to Delta Dental Bellwether Defendants had she known of their inadequate and lax data security policies and practices.

633. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Delta Dental of California and affiliates' possession, is protected and safeguarded from future breaches.

634. As a direct and proximate result of the Data Breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her financial accounts and credit to reduce the risk of future identity theft and fraud.

635. To date, as a result of the Data Breach, Plaintiff has spent several hours researching the details and checking her credit and financial accounts for any unauthorized and suspicious activity, a practice that Plaintiff will need to continue indefinitely to protect against and/or remedy fraud and identity theft.

636. Had Delta Dental of California and affiliates not delayed in notifying her about the Data Breach, she could have taken precautions earlier on to protect her identity and mitigate the harms of the Data Breach.

637. As a result of the Data Breach, Plaintiff anticipates spending considerable money and additional time on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She faced and continues to a face risk of fraud and identity theft presently that will last for her lifetime.

638. Plaintiff suffered lost time, annoyance, interference, inconvenience, and incurred expenses as a result of the Data Breach.

639. Had Plaintiff been informed that Delta Dental Bellwether Defendants had insufficient data security measures to protect her Private Information, she would have taken this into account in deciding whether to enroll in Delta Dental insurance, and, at a minimum, Plaintiff would not have paid as much for dental insurance.

640. Plaintiff relied on Delta Dental Bellwether Defendants' policies and promises to implement sufficient regulatory and industry compliant measures to protect her Private Information and privacy rights.

641. Due to the highly sensitive nature of the stolen information and its unauthorized dissemination, Plaintiff has already suffered harm, including damages and a loss in the value of her Private Information—an intangible asset entrusted to the Delta Dental Bellwether Defendants. Plaintiff also faces a substantial and imminent risk of future harm.

14. Yvette Tillman

642. Plaintiff Yvette Tillman is, and at all times mentioned herein was, an individual citizen of the State of South Carolina, residing in Ladson, South Carolina.

643. Plaintiff is a current customer of DDIC and was a customer at the time of the Data Breach. Plaintiff receives Delta Dental insurance through her employer.

644. Plaintiff Tillman provided her Private Information to Delta Dental Bellwether Defendants as a condition of receiving dental insurance.

645. Plaintiff Tillman had the reasonable expectation and understanding that Delta Dental Bellwether Defendants would take—at minimum—industry standard precautions to protect, maintain, and safeguard that highly sensitive information from unauthorized users or disclosure, and would timely notify her of any data security incidents. Plaintiff would not have entrusted her Private Information to Delta Dental Bellwether Defendants had she known that Delta Dental Bellwether Defendants would not take reasonable steps to safeguard her information.

646. Plaintiff Tillman received a letter from "Delta Dental of California and affiliates" (referred to in the Notice Letter as "Company") dated February 9, 2024 concerning the Data Breach. The letter explained that cybercriminals exploited a security vulnerability in the systems of one of Delta Dental of California and affiliates' third-party vendors, Progress. As a result, unauthorized individuals accessed or obtained data stored on the platform, including the Plaintiff's information. The letter further states the following:

> **What Happened?**
>
> Progress Software announced a previously unknown vulnerability within their widely used MOVEit file-transfer software program. This vulnerability led to a global data security incident that is reported to have impacted many organizations, including corporations, government agencies, insurance providers, pension funds, financial institutions, state education systems and more. On June 1, 2023, the Company learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application. Immediately after being alerted of the incident, we launched a thorough investigation and took steps to contain and remediate the incident. We stopped access to the MOVEit software, removed the malicious files, conducted a thorough analysis of the MOVEit database, applied the recommended patches, and reset administrative passwords to the MOVEit system. We also enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity, and ransomware activity. On July 6, 2023,

> our investigation confirmed that the Company information on the MOVEit platform had been accessed and acquired without authorization between May 27, 2023 and May 30, 2023. At that time, we promptly engaged independent third-party experts in computer forensics, analytics, and data mining to determine what information was impacted and with whom it is associated. This extensive investigation and analysis of the data recently concluded and was a critical component in enabling us to identify specific personal information that was acquired from the MOVEit platform. Upon that determination, we have worked diligently to identify any impacted individuals to provide notification. On November 27, 2023, we determined your personal information was affected. In addition to our own investigation, we have also notified law enforcement of the incident and have been cooperating with them since.
>
> **What Information Was Involved?** Your affected information included date of birth and health insurance information**.**

647. Since the Data Breach, including prior to being notified by Delta Dental of California and affiliates that her Private Information had been compromised and in the hands of cybercriminals, Plaintiff has experienced an increase in the amount of intrusive spam calls, texts, and emails she receives.

648. Since the Data Breach, Plaintiff Tillman discovered several fraudulent charges on her Chase Bank debit card which amounted to $1,000 in September and October 2023. Plaintiff was also alerted that someone applied for a credit card in her name and that there had been multiple hard inquiries into her credit due to fraudulent activity.

649. Upon information and belief, Plaintiff's unencrypted Private Information was viewed by unauthorized persons, as evidenced by the fraudulent activity and other suspicious charges to her accounts and that Plaintiff has experienced an uptick in phishing emails since the Data Breach, among other harms described.

650. The disclosure of her health insurance information is highly offensive due to the deeply personal nature of health and medical data. This Data Breach has caused her significant anxiety, increased concerns about the loss of privacy, and fears over the potential misuse of her

sensitive information by cybercriminals. She now faces a serious risk of identity theft, credit fraud, and other potential harms, both at present and in the future.

651. Plaintiff Tillman values her privacy and is very careful about storing and sharing sensitive Private Information. Plaintiff would not have entrusted her Private Information to Delta Dental Bellwether Defendants had she known of their inadequate and lax data security policies and practices.

652. Plaintiff Tillman has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Delta Dental of California and affiliates' possession, is protected and safeguarded from future breaches.

653. As a direct and proximate result of the Data Breach, Plaintiff Tillman has made reasonable efforts to mitigate the impact of the Data Breach, including by investigating fraudulent and suspicious activity she experienced, contacting banks, credit card companies, or other vendors about the suspicious, fraudulent activity she experienced, expending time to get fraudulent charges reversed, and by regularly and closely monitoring her financial accounts to reduce the risk of future identity theft and fraud.

654. To date, as a result of the Data Breach, Plaintiff Tillman has spent about 90 hours researching the details of the Data Breach and performing the aforementioned tasks to mitigate the impact of the Data Breach. Plaintiff Tillman will need to continue the practice of checking her credit and financial accounts for any unauthorized, suspicious activity to protect against and/or remedy fraud and identity theft for the rest of her life.

655. Had Delta Dental of California and affiliates not delayed in notifying Plaintiff about the Data Breach, she could have taken additional precautions earlier on to protect her identity and mitigate the harms of the Data Breach.

656. As a result of the Data Breach, Plaintiff Tillman anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She has faced and continues to face a risk of fraud and identity theft that will last for her lifetime.

657. Plaintiff Tillman suffered lost time, annoyance, interference, inconvenience as well as money as a result of the Data Breach.

658. Had Plaintiff Tillman been informed that Delta Dental Bellwether Defendants had insufficient data security measures to protect her Private Information, she would have taken this into account in deciding whether to enroll in Delta Dental insurance, and, at a minimum, Plaintiff would not have paid as much for dental insurance.

659. Plaintiff Tillman relied on Delta Dental Bellwether Defendants' policies and promises to implement sufficient regulatory and industry compliant measures to protect her Private Information and privacy rights.

660. Due to the highly sensitive nature of the stolen information and its unauthorized dissemination, Plaintiff has already suffered harm, including damages and a loss in the value of her Private Information—an intangible asset entrusted to the Delta Dental Bellwether Defendants. Plaintiff also faces a substantial and imminent risk of future harm.

D. PBI Bellwether Plaintiffs

1. PBI Bellwether Plaintiffs Alleging Claims Against Genworth Defendants

a. Plaintiff Keith Bailey

661. Plaintiff **Keith Bailey** ("Plaintiff Bailey") is a resident and citizen of the state of Florida and resides in Naples, Florida.

662. Plaintiff Bailey has a long-term insurance policy with Genworth.

663. Plaintiff Bailey received a letter directly from Genworth dated July 31, 2023, which reported that "Genworth was recently notified by [PBI] that your personal information was involved in a data security event that took advantage of a vulnerability in the widely-used MOVEit file transfer software that PBI uses." The letter further states:

> PBI is a third-party vendor that Genworth uses to satisfy regulatory obligations to scan various databases to determine whether a customer may have passed and triggered death benefits under a life insurance policy or annuity contract. We also use PBI to identify deaths that have occurred across our other lines of insurance, as well as the deaths of insurance agents to whom we pay commissions.

664. At the time that Progress discovered the data breach—on or around May 31, 2023—Progress, PBI, and Genworth retained Plaintiff Bailey's PII in their computer systems.

665. Accordingly, the letter states that Progress, PBI, and Genworth possessed Plaintiff Bailey's PII but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

666. According to the letter, Progress, PBI, and Genworth learned of the Data Breach as early as May 29-31, 2023, but they waited approximately two months before Genworth notified Plaintiff Bailey that his highly sensitive PII was compromised in the Data Breach.

667. In addition to their substantial delay in notifying Plaintiff Bailey of the Data Breach, Progress, PBI, and Genworth also put the burden on Plaintiff Bailey to prevent any further harm resulting from the Data Breach by stating in the letter: "Please watch for a letter from PBI in an envelope with the PBI logo with [credit monitoring] activation instructions" and "You can visit [Genworth's website] for up-to-date FAQs on the security event and Genworth's response, as well as tips on protecting your identity."

668. According to the letter, Progress, PBI, and Genworth waited two months before they notified Plaintiff Bailey that his PII was compromised in the Data Breach. To date, critical

details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Bailey, who retains a vested interest in ensuring that his PII remains protected.

669. Moreover, Genworth's disclosure of the Breach amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Bailey of the Data Breach's critical facts.

670. As a direct and proximate result of the Data Breach, Plaintiff Bailey spent time, approximately 30 hours, registering for Kroll credit monitoring, researching the Breach, contacting Genworth about the Breach, and monitoring accounts for suspicious activity.

671. Plaintiff Bailey greatly values his privacy and PII and takes reasonable steps to maintain the confidentiality of his PII. Plaintiff Bailey is very careful about sharing his PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Bailey stores any and all documents containing PII in a secure location and destroys any documents he receives in the mail that contain any PII or any information that could otherwise be used to compromise his identity and/or credit. Moreover, Plaintiff Bailey diligently chooses unique usernames and passwords for his various online accounts, and he takes steps to ensure his online accounts are secure and password protected.

672. Plaintiff Bailey is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud, resulting from the Data Breach. The Data Breach has caused Plaintiff Bailey to suffer anger and stress, which have been compounded by the two-month delay by Progress, PBI, and Genworth in informing him of the fact that his PII was acquired by known cybercriminals through the Data Breach.

673. Plaintiff Bailey anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Bailey will continue to be at present and continued increased risk of identity theft and fraud for years to come.

674. Plaintiff Bailey has a continuing interest in ensuring that his PII, which remains in Progress, PBI, and Genworth's possession, is protected and safeguarded from future disclosure and/or data breaches.

675. Moreover, when Plaintiff Bailey purchased insurance from Genworth, he did not receive the benefit of the bargain because, had he known that Progress, PBI, and Genworth were using substandard data security policies, he would not have purchased or would have paid less for the Genworth insurance policy.

676. As a result of the Data Breach, Plaintiff Bailey has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of his stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of his personal data; lost property in the form of his compromised PII; and injury to his privacy. Additionally, as a direct result of the Data Breach, Plaintiff Bailey now faces a substantial risk that unauthorized third parties will further misuse his PII because (1) the Data Breach involved a single cybercriminal organization, Cl0p, specifically targeting Defendants' systems; (2) the dataset of PII that Cl0p exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PII Cl0p exfiltrated in the Data Breach is highly sensitive

and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Bailey has (1) suffered, or is at an increased risk of suffering, unauthorized use of his stolen PII such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm because he lost time that he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort he expended addressing future consequences of the Data Breach.

677. Plaintiff Bailey experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Bailey would compensate him for the foregoing redressable injuries. Further, Plaintiff Bailey seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of his PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

b. Plaintiff Camille Burgan

678. Plaintiff Camille Burgan ("Plaintiff Camille Burgan") is citizen of the state of California and resides in San Ysidro, California.

679. Plaintiff Camille Burgan is a former life insurance policyholder with Genworth. She purchased the policy and provided her PII to Genworth from her residence in California.

680. Plaintiff Camille Burgan received a letter directly from Genworth dated July 31, 2023, which reported that "Genworth was recently notified by [PBI] that your personal information

was involved in a data security event that took advantage of a vulnerability in the widely-used MOVEit file transfer software that PBI uses." The letter further states:

> PBI is a third-party vendor that Genworth uses to satisfy regulatory obligations to scan various databases to determine whether a customer may have passed and triggered death benefits under a life insurance policy or annuity contract. We also use PBI to identify deaths that have occurred across our other lines of insurance, as well as the deaths of insurance agents to whom we pay commissions.

681. 10 days prior, Plaintiff Camille Burgan received a letter from PBI dated July 21, 2023, which states that PBI "provides audit and address research services for insurance companies, pension funds, and other organizations, including Genworth Life Insurance Company (GLIC), or for a third party acting on their behalf" and experienced the Data Breach, which "affected the security of some of [Plaintiff Camille Burgan's] information." The letter states further as follows:

> **What Happened?** On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded your data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.
>
> **What Information Was Involved?** Our investigation determined that the following types of information related to you were present in the server at the time of the event: name, Social Security number, date of birth, zip code, state of residence, role in policy/account (e.g., Annuitant, Joint Insured, Owner, etc.), general product type, and policy/account number.

682. At the time that Progress discovered the data breach—on or around May 31, 2023—Progress, PBI, and Genworth retained Plaintiff Camille Burgan's PII in their computer systems.

683. Accordingly, the letter states that Progress, PBI, and Genworth possessed Plaintiff Camille Burgan's PII, including her name, Social Security number, date of birth, zip code, state of residence, role in policy/account (e.g., Annuitant, Joint Insured, Owner, etc.), general product type,

and policy/account number, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

684. According to the letter, Progress, PBI, and Genworth learned of the Data Breach as early as May 29-31, 2023 but they waited approximately two months before Genworth notified Plaintiff Camille Burgan that her highly sensitive PII was compromised in the Data Breach.

685. In addition to their substantial delay in notifying Plaintiff Camille Burgan of the Data Breach, Progress, PBI, and Genworth also put the burden on Plaintiff Camille Burgan to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors . . . and to report suspected identity theft incidents to the insurance company."

686. According to the letter, Progress, PBI, and Genworth waited two months before they notified Plaintiff Camille Burgan that her PII was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Camille Burgan, who retains a vested interest in ensuring that her PII remains protected.

687. Moreover, Genworth's disclosure of the Breach amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Camille Burgan of the Data Breach's critical facts.

688. Plaintiff Camille Burgan's PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. As a direct and proximate result of the Data Breach, Plaintiff Camille Burgan has encountered an increase in spam/phishing calls, emails, and text messages. As a direct and proximate result of the Data Breach, Plaintiff Camille Burgan spent

time, approximately 60 hours, renewing her Identity Guard credit and identity monitoring, researching the Breach, contacting Genworth about the Breach, and monitoring accounts for suspicious activity. Furthermore, Plaintiff Camille Burgan has incurred out-of-pocket expenses as a result of the Data Breach, including paid credit/identity theft monitoring services.

689. Plaintiff Camille Burgan greatly values her privacy and PII and takes reasonable steps to maintain the confidentiality of her PII. Plaintiff Camille Burgan is very careful about sharing her PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Camille Burgan stores any and all documents containing PII in a secure location and destroys any documents she receives in the mail that contain any PII or any information that could otherwise be used to compromise her identity and/or credit. Moreover, Plaintiff Camille Burgan diligently chooses unique usernames and passwords for her various online accounts, and she takes steps to ensure her online accounts are secure and password protected.

690. Plaintiff Camille Burgan is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud, resulting from the Data Breach. The Data Breach has caused Plaintiff Camille Burgan to suffer anxiety, rage, anger, and stress, which have been compounded by Progress, PBI, and Genworth's two-month delay in informing her of the fact that her PII, including her Social Security number, was acquired by known cybercriminals through the Data Breach.

691. Plaintiff Camille Burgan anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Camille Burgan will continue to be at present and continued increased risk of identity theft and fraud for years to come.

692. Plaintiff Camille Burgan has a continuing interest in ensuring that her PII, which remains in Progress's, PBI's, and Genworth's possession, is protected and safeguarded from future disclosure and/or data breaches.

693. Moreover, when Plaintiff Camille Burgan purchased life insurance from Genworth, she did not receive the benefit of the bargain because, had she known that Progress, PBI, and Genworth were using substandard data security policies, she would not have purchased or would have paid less for the Genworth life insurance policy.

694. As a result of the Data Breach, Plaintiff Camille Burgan has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised PII; and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff Camille Burgan now faces a substantial risk that unauthorized third parties will further misuse her PII because (1) the Data Breach involved a single cybercriminal organization, Cl0p, specifically targeting Defendants' systems; (2) the dataset of PII that Cl0p exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PII Cl0p exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Camille Burgan has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen PII such that she

has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time that she spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

695. Plaintiff Camille Burgan experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Camille Burgan would compensate her for the foregoing redressable injuries. Further, Plaintiff Camille Burgan seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of her PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

c. Plaintiff Eugene Burgan

696. Plaintiff Eugene Burgan ("Plaintiff Eugene Burgan") is citizen of the state of California and resides in San Ysidro, California.

697. Plaintiff Eugene Burgan is a former life insurance policyholder with Genworth. He purchased the policy and provided his PII to Genworth from his residence in California.

698. Plaintiff Eugene Burgan received a letter directly from Genworth dated July 31, 2023, which reported that "Genworth was recently notified by [PBI] that your personal information was involved in a data security event that took advantage of a vulnerability in the widely-used MOVEit file transfer software that PBI uses." The letter further states:

> PBI is a third-party vendor that Genworth uses to satisfy regulatory obligations to scan various databases to determine whether a customer may have passed and triggered death benefits under a life insurance policy or annuity contract. We also

> use PBI to identify deaths that have occurred across our other lines of insurance, as well as the deaths of insurance agents to whom we pay commissions.

699. 10 days prior, Plaintiff Eugene Burgan received a letter from PBI dated July 21, 2023, which states that PBI "provides audit and address research services for insurance companies, pension funds, and other organizations, including Genworth Life Insurance Company (GLIC), or for a third party acting on their behalf" and experienced the Data Breach, which "may affect the security of some of [Plaintiff Eugene Burgan's] information." The letter states further as follows:

> **What Happened?** On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded your data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.
>
> **What Information Was Involved?** Our investigation determined that the following types of information related to you were present in the server at the time of the event: name, Social Security number, date of birth, zip code, state of residence, role in policy/account (e.g., Annuitant, Joint Insured, Owner, etc.), general product type, and policy/account number.

700. At the time that Progress discovered the data breach—on or around May 31, 2023—Progress, PBI, and Genworth retained Plaintiff Eugene Burgan's PII in their computer systems.

701. Accordingly, the letter states that Progress, PBI, and Genworth possessed Plaintiff Eugene Burgan's PII, including his name, Social Security number, date of birth, zip code, state of residence, role in policy/account (e.g., Annuitant, Joint Insured, Owner, etc.), general product type, and policy/account number, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

702. According to the letter, Progress, PBI, and Genworth learned of the Data Breach as early as May 29-31, 2023, but they waited approximately two months before Genworth notified Plaintiff Eugene that his highly sensitive PII was compromised in the Data Breach.

703. In addition to their substantial delay in notifying Plaintiff Eugene Burgan of the Data Breach, Progress, PBI, and Genworth also put the burden on Plaintiff Eugene Burgan to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors . . . and to report suspected identity theft incidents to the insurance company."

704. According to the letter, Progress, PBI, and Genworth waited two months before they notified Plaintiff Eugene Burgan that his PII was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Eugene Burgan, who retains a vested interest in ensuring that his PII remains protected.

705. Moreover, Genworth's disclosure of the Breach amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Eugene Burgan of the Data Breach's critical facts.

706. Plaintiff Eugene Burgan's PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. As a direct and proximate result of the Data Breach, Plaintiff Eugene Burgan has encountered an increase in spam/phishing calls, emails, and text messages. Additionally, Plaintiff Eugene Burgan received a notification, reporting that his PII was detected on the Dark Web. As a direct and proximate result of the Data Breach, Plaintiff Eugene Burgan spent time monitoring his accounts for suspicious activity. Furthermore, Plaintiff

Eugene Burgan has incurred out-of-pocket expenses as a result of the Data Breach, including paid credit/identity theft monitoring services.

707. Plaintiff Eugene Burgan greatly values his privacy and PII and takes reasonable steps to maintain the confidentiality of his PII. Plaintiff Eugene Burgan is very careful about sharing his PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Eugene Burgan stores any and all documents containing PII in a secure location and destroys any documents he receives in the mail that contain any PII or any information that could otherwise be used to compromise his identity and/or credit. Moreover, Plaintiff Eugene Burgan diligently chooses unique usernames and passwords for his various online accounts, and he takes steps to ensure his online accounts are secure and password-protected.

708. Plaintiff Eugene Burgan is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud, resulting from the Data Breach. The Data Breach has caused Plaintiff Eugene Burgan to suffer fear, anxiety, anger, and stress, which have been compounded by Progress, PBI, and Genworth's two-month delay in informing him of the fact that his PII, including his Social Security number, was acquired by known cybercriminals through the Data Breach.

709. Plaintiff Eugene Burgan anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Eugene Burgan will continue to be at present and continued increased risk of identity theft and fraud for years to come.

710. Plaintiff Eugene Burgan has a continuing interest in ensuring that his PII, which remains in Progress, PBI, and Genworth's possession, is protected and safeguarded from future disclosure and/or data breaches.

711. Moreover, when Plaintiff Eugene Buran purchased life insurance from Genworth, he did not receive the benefit of the bargain because, had he known that Progress, PBI, and Genworth were using substandard data security policies, he would not have purchased or would have paid less for the Genworth life insurance policy.

712. As a result of the Data Breach, Plaintiff Eugene Burgan has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of his stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of his personal data; lost property in the form of his compromised PII; and injury to his privacy. Additionally, as a direct result of the Data Breach, Plaintiff Eugene Burgan now faces a substantial risk that unauthorized third parties will further misuse his PII because (1) the Data Breach involved a single cybercriminal organization, Cl0p, specifically targeting Defendants' systems; (2) the dataset of PII that Cl0p exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PII Cl0p exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Eugene Burgan has (1) suffered, or is at an increased risk of suffering, unauthorized use of his stolen PII such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm because he lost time that he spent

taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort he expended addressing future consequences of the Data Breach.

713. Plaintiff Eugene Burgan experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Eugene Burgan would compensate him for the foregoing redressable injuries. Further, Plaintiff Eugene Burgan seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of his PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

d. Plaintiff Gilbert Hale

714. Plaintiff Gilbert Hale ("Plaintiff Gilbert Hale") is a resident and citizen of the state of New York and resides in Pittsford, New York.

715. Plaintiff Gilbert Hale holds a life insurance policy with Genworth. He purchased the policy and provided his PII to Genworth from his residence in New York.

716. Plaintiff Gilbert Hale received a letter directly from Genworth dated July 31, 2023, which reported that "Genworth was recently notified by [PBI] that your personal information was involved in a data security event that took advantage of a vulnerability in the widely used MOVEit file transfer software that PBI uses." The letter further states:

> PBI is a third-party vendor that Genworth uses to satisfy regulatory obligations to scan various databases to determine whether a customer may have passed and triggered death benefits under a life insurance policy or annuity contract. We also use PBI to identify deaths that have occurred across our other lines of insurance, as well as the deaths of insurance agents to whom we pay commissions.

717. At the time that Progress discovered the data breach—on or around May 31, 2023—Progress, PBI and Genworth retained Plaintiff Gilbert Hale's PII in their computer systems.

718. Accordingly, the letter states that PBI and Genworth possessed Plaintiff Gilbert Hale's PII but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

719. According to the letter, Progress, PBI, and Genworth learned of the Data Breach as early as May 29-31, 2023, but they waited approximately two months before Genworth notified Plaintiff Gilbert Hale that his highly sensitive PII was compromised in the Data Breach.

720. In addition to their substantial delay in notifying Plaintiff Gilbert Hale of the Data Breach, Progress, PBI and Genworth also put the burden on Plaintiff Gilbert Hale to prevent any further harm resulting from the Data Breach by stating in the letter: "Please watch for a letter from PBI in an envelope with the PBI logo with [credit monitoring] activation instructions" and "You can visit [Genworth's website] for up-to-date FAQs on the security event and Genworth's response, as well as tips on protecting your identity."

721. According to the letter, Progress, PBI and Genworth waited two months before they notified Plaintiff Gilbert Hale that his PII was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Gilbert Hale, who retains a vested interest in ensuring that his PII remains protected.

722. Moreover, Genworth's disclosure of the Breach amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Gilbert Hale of the Data Breach's critical facts.

723. Plaintiff Gilbert Hale's PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. On March 27, 2024, Plaintiff Gilbert Hale received an email from Capital One, stating that it detected suspicious activity on his wife, Lynda

Hale's Quick Silver Capital One credit card and that it restricted the card from making any further transactions. Additionally, Plaintiff Gilbert Hale received a notification, reporting that his PII was detected on the Dark Web. As a direct and proximate result of the Data Breach, Plaintiff Gilbert Hale spent time registering for free credit monitoring services. Further, he spent time, approximately 300 to 400 hours, researching the Breach, contacting the card issuer to preemptively get new account numbers issued, monitoring accounts for suspicious activity, investigating fraudulent/suspicious activity, freezing his credit, registering for free credit monitoring services, and contacting banks, credit card companies, or other vendors about fraudulent/suspicious activity.

724. Plaintiff Gilbert Hale greatly values his privacy and PII and takes reasonable steps to maintain the confidentiality of his PII. Plaintiff Gilbert Hale is very careful about sharing his PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Gilbert Hale stores any and all documents containing PII in a secure location and destroys any documents he receives in the mail that contain any PII or any information that could otherwise be used to compromise his identity and/or credit. Moreover, Plaintiff Gilbert Hale diligently chooses unique usernames and passwords for his various online accounts, and he takes steps to ensure his online accounts are secure and password-protected.

725. Plaintiff Gilbert Hale is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud, resulting from the Data Breach. The Data Breach has caused Plaintiff Gilbert Hale to suffer fear, anxiety, rage, anger, and stress, which have been compounded by Progress, PBI and Genworth's two-month delay in informing him of the fact that his PII was acquired by known cybercriminals through the Data Breach.

726. Plaintiff Gilbert Hale anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff

Gilbert Hale will continue to be at present and continued increased risk of identity theft and fraud for years to come.

727. Plaintiff Gilbert Hale has a continuing interest in ensuring that his PII, which remains in Progress, PBI and Genworth's possession, is protected and safeguarded from future disclosure and/or data breaches.

728. Moreover, when Plaintiff Gilbert Hale purchased life insurance from Genworth, he did not receive the benefit of the bargain because, had he known that Progress, PBI and Genworth were using substandard data security policies, he would not have purchased or would have paid less for the Genworth life insurance policy.

729. As a result of the Data Breach, Plaintiff Gilbert Hale has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of his stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of his personal data; lost property in the form of his compromised PII; and injury to his privacy. Additionally, as a direct result of the Data Breach, Plaintiff Gilbert Hale now faces a substantial risk that unauthorized third parties will further misuse his PII because (1) the Data Breach involved a single cybercriminal organization, Cl0p, specifically targeting Defendants' systems; (2) the dataset of PII that Cl0p exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PII Cl0p exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial

accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Gilbert Hale has (1) suffered, or is at an increased risk of suffering, unauthorized use of his stolen PII such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm because he lost time that he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort he expended addressing future consequences of the Data Breach.

730. Plaintiff Gilbert Hale experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Gilbert Hale would compensate him for the foregoing redressable injuries. Further, Plaintiff Gilbert Hale seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of his PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

e. Plaintiff Lynda Hale

731. Plaintiff Lynda Hale ("Plaintiff Lynda Hale") is a resident and citizen of the state of New York and resides in Pittsford, New York.

732. Plaintiff Lynda Hale holds a life insurance policy with Genworth. She purchased the policy and provided her PII to Genworth from her residence in New York.

733. Plaintiff Lynda Hale received a letter directly from Genworth dated July 31, 2023, which reported that "Genworth was recently notified by [PBI] that your personal information was involved in a data security event that took advantage of a vulnerability in the widely used MOVEit file transfer software that PBI uses." The letter further states:

> PBI is a third-party vendor that Genworth uses to satisfy regulatory obligations to scan various databases to determine whether a customer may have passed and triggered death benefits under a life insurance policy or annuity contract. We also use PBI to identify deaths that have occurred across our other lines of insurance, as well as the deaths of insurance agents to whom we pay commissions.

734. At the time that Progress discovered the data breach—on or around May 31, 2023—Progress, PBI and Genworth retained Plaintiff Lynda Hale's PII in their computer systems.

735. Accordingly, the letter states that PBI and Genworth possessed Plaintiff Lynda Hale's PII but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

736. According to the letter, Progress, PBI, and Genworth learned of the Data Breach as early as May 29-31, 2023, but they waited approximately two months before Genworth notified Plaintiff Lynda Hale that her highly sensitive PII was compromised in the Data Breach.

737. In addition to their substantial delay in notifying Plaintiff Lynda Hale of the Data Breach, Progress, PBI and Genworth also put the burden on Plaintiff Lynda Hale to prevent any further harm resulting from the Data Breach by stating in the letter: "Please watch for a letter from PBI in an envelope with the PBI logo with [credit monitoring] activation instructions" and "You can visit [Genworth's website] for up-to-date FAQs on the security event and Genworth's response, as well as tips on protecting your identity."

738. According to the letter, Progress, PBI and Genworth waited two months before they notified Plaintiff Lynda Hale that her PII was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Lynda Hale, who retains a vested interest in ensuring that her PII remains protected.

739. Moreover, Genworth's disclosure of the Breach amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Lynda Hale of the Data Breach's critical facts.

740. Plaintiff Lynda Hale's PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. In March 2024, Plaintiff Lynda Hale's Quick Silver Capital One credit card incurred fraudulent/suspicious activity. Capital One issued a replacement card and removed the fraudulent charge. On October 26, 2024, Plaintiff Lynda Hale attempted to place an online order on InstaCart, and she received a notification that the account was locked as a result of fraudulent/suspicious activity. Furthermore, as a direct and proximate result of the Data Breach, Plaintiff Lynda Hale has experienced an increase in spam/phishing emails. As a direct and proximate result of the Data Breach, Plaintiff Lynda Hale has spent time, approximately five hours, monitoring accounts for fraudulent/suspicious activity, and investigating fraudulent activity.

741. Plaintiff Lynda Hale greatly values her privacy and PII and takes reasonable steps to maintain the confidentiality of her PII. Plaintiff Lynda Hale is very careful about sharing her PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Lynda Hale stores any and all documents containing PII in a secure location and destroys any documents she receives in the mail that contain any PII or any information that could otherwise be used to compromise her identity and/or credit. Moreover, Plaintiff Lynda Hale diligently chooses unique usernames and passwords for her various online accounts, and she takes steps to ensure her online accounts are secure and password-protected.

742. Plaintiff Lynda Hale is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud, resulting from the Data Breach. The Data Breach

has caused Plaintiff Lynda Hale to suffer fear, anxiety, anger, rage, and stress, which have been compounded by Progress, PBI and Genworth's two-month delay in informing her of the fact that her PII was acquired by known cybercriminals through the Data Breach.

743. Plaintiff Lynda Hale anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Lynda Hale will continue to be at present and continued increased risk of identity theft and fraud for years to come.

744. Plaintiff Lynda Hale has a continuing interest in ensuring that her PII, which remains in Progress, PBI and Genworth's possession, is protected and safeguarded from future disclosure and/or data breaches.

745. Moreover, when Plaintiff Lynda Hale purchased life insurance from Genworth, she did not receive the benefit of the bargain because, had she known that Progress, PBI and Genworth were using substandard data security policies, she would not have purchased or would have paid less for the Genworth life insurance policy.

746. As a result of the Data Breach, Plaintiff Lynda Hale has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised PII; and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff Lynda Hale now faces a substantial risk that unauthorized third parties will further misuse her PII because (1) the Data Breach involved a single

cybercriminal organization, Cl0p, specifically targeting Defendants' systems; (2) the dataset of PII that Cl0p exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PII Cl0p exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Lynda Hale has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen PII such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time that he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

747. Plaintiff Lynda Hale experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Lynda Hale would compensate him for the foregoing redressable injuries. Further, Plaintiff Lynda Hale seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of her PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

f. Plaintiff Brinitha Harris

748. Plaintiff Brinitha Harris ("Plaintiff Harris") is a resident and citizen of the state of California and resides in Palmdale, California.

749. Plaintiff Harris holds a life insurance policy with Genworth.

750. Plaintiff Harris received a letter directly from Genworth dated July 31, 2023, which reported that "Genworth was recently notified by [PBI] that your personal information was involved in a data security event that took advantage of a vulnerability in the widely-used MOVEit file transfer software that PBI uses." The letter further states:

> PBI is a third-party vendor that Genworth uses to satisfy regulatory obligations to scan various databases to determine whether a customer may have passed and triggered death benefits under a life insurance policy or annuity contract. We also use PBI to identify deaths that have occurred across our other lines of insurance, as well as the deaths of insurance agents to whom we pay commissions.

751. At the time that Progress discovered the data breach—on or around May 31, 2023—Progress, PBI, and Genworth retained Plaintiff Harris's PII in their computer systems.

752. Accordingly, the letter states that Progress, PBI, and Genworth possessed Plaintiff Harris's PII, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

753. According to the letter, Progress, PBI, and Genworth learned of the Data Breach as early as May 29-31, 2023, but they waited approximately two months before Genworth notified Plaintiff Harris that her highly sensitive PII was compromised in the Data Breach.

754. In addition to their substantial delay in notifying Plaintiff Harris of the Data Breach, Progress, PBI, and Genworth also put the burden on Plaintiff Harris to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors . . . and to report suspected identity theft incidents to the institution."

755. According to the letter, Progress, PBI, and Genworth waited two months before they notified Plaintiff Harris that her PII was compromised in the Data Breach. To date, critical

details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Harris, who retains a vested interest in ensuring that her PII remains protected.

756. Moreover, Genworth's disclosure of the Breach amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Harris of the Data Breach's critical facts.

757. Plaintiff Harris's PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. In November 2023, Plaintiff Harris discovered that someone fraudulently opened an account for electric utilities in her name. On or around November 2024, Plaintiff Harris discovered that someone opened a Wells Fargo bank account in her name. Also in 2024, she discovered that someone opened a US Bank account in her name. Moreover, Plaintiff Harris has experienced in increase in spam/phishing calls, emails, and text messages. As a direct and proximate result of the Data Breach, Plaintiff Harris spent time totaling approximately 35 hours investigating the fraudulent/suspicious activity alleged above, contacting US Bank and Wells Fargo to dispute the fraudulent opening of bank accounts in her name, contacting the electric utilities company to close the fraudulent account opened in her name, and gathering documents and taking other steps to prove that she did not open any of those fraudulent accounts.

758. Plaintiff Harris greatly values her privacy and PII and takes reasonable steps to maintain the confidentiality of her PII. Plaintiff Harris is very careful about sharing her PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Harris stores any and all documents containing PII in a secure location and destroys any documents her receives in the mail that contain any PII or any information that could otherwise be used to compromise her identity and/or credit. Moreover, Plaintiff Harris diligently chooses unique

usernames and passwords for her various online accounts, and her takes steps to ensure her online accounts are secure and password-protected.

759. Plaintiff Harris is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud, resulting from the Data Breach. The Data Breach has caused Plaintiff Harris to suffer fear, anxiety, sleep disruption, rage, anger, physical pain, and stress, which has been compounded by Progress, PBI, and Genworth's two-month delay in informing her of the fact that her PII, including her Social Security number, was acquired by known cybercriminals through the Data Breach.

760. Plaintiff Harris anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Harris will continue to be at present and continued increased risk of identity theft and fraud for years to come.

761. Plaintiff Harris has a continuing interest in ensuring that her PII, which remains in Progress, PBI, and Genworth's possession, is protected and safeguarded from future disclosure and/or data breaches.

762. As a result of the Data Breach, Plaintiff Harris has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised PII; and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff Harris now faces a substantial risk that unauthorized third

parties will further misuse her PII because (1) the Data Breach involved a single cybercriminal organization, Cl0p, specifically targeting Defendants' systems; (2) the dataset of PII that Cl0p exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PII Cl0p exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Harris has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen PII such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because her lost time that her spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort her expended addressing future consequences of the Data Breach.

763. Plaintiff Harris experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Harris would compensate her for the foregoing redressable injuries. Further, Plaintiff Harris seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of her PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

g. Plaintiff Patrice Hauser

764. Plaintiff Patrice Hauser ("Plaintiff Hauser") is a resident and citizen of the state of Florida and resides in Lakewood Ranch, Florida.

765. Plaintiff Hauser is currently a resident and citizen of the state of Florida and holds a life insurance policy with Genworth that she purchased from her former residence in North Carolina.

766. Plaintiff Hauser received a letter directly from Genworth at her address in Florida dated July 31, 2023, which reported that "Genworth was recently notified by [PBI] that your personal information was involved in a data security event that took advantage of a vulnerability in the widely-used MOVEit file transfer software that PBI uses." The letter further states:

> PBI is a third-party vendor that Genworth uses to satisfy regulatory obligations to scan various databases to determine whether a customer may have passed and triggered death benefits under a life insurance policy or annuity contract. We also use PBI to identify deaths that have occurred across our other lines of insurance, as well as the deaths of insurance agents to whom we pay commissions.

767. 17 days prior, Plaintiff Hauser received a letter from PBI at her address in Florida dated July 14, 2023, which states that PBI "provides audit and address research services for insurance companies, pension funds, and other organizations, including Genworth Life Insurance Company (GLIC), or for a third party acting on their behalf" and experienced the Data Breach, which "affected the security of some of [Plaintiff Hauser's] information." The letter states further as follows:

> **What Happened?** On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded your data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.
>
> **What Information Was Involved?** Our investigation determined that the following types of information related to you were present in the server at the time of the event: name, Social Security number, date of birth, zip code, state of

residence, role in policy/account (e.g., Annuitant, Joint Insured, Owner, etc.), general product type, and policy/account number.

768. At the time that Progress discovered the data breach—on or around May 31, 2023—Progress, PBI, and Genworth retained Plaintiff Hauser's PII in their computer systems.

769. Accordingly, the letter states that Progress, PBI, and Genworth possessed Plaintiff Hauser's PII, including her name, Social Security number, date of birth, zip code, state of residence, role in policy/account (e.g., Annuitant, Joint Insured, Owner, etc.), general product type, and policy/account number, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

770. According to the letter, Progress, PBI, and Genworth learned of the Data Breach as early as May 29-31, 2023, but they waited approximately two months before PBI and Genworth notified Plaintiff Hauser that her highly sensitive PII was compromised in the Data Breach.

771. In addition to their substantial delay in notifying Plaintiff Hauser of the Data Breach, Progress, PBI, and Genworth also put the burden on Plaintiff Hauser to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors . . . and to report suspected identity theft incidents to the insurance company."

772. According to the letter, Progress, PBI, and Genworth waited approximately two months before they notified Plaintiff Hauser that her PII was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Hauser, who retains a vested interest in ensuring that her PII remains protected.

773. Moreover, PBI and Genworth's disclosure of the Breach amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Hauser of the Data Breach's critical facts.

774. Plaintiff Hauser's PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. Plaintiff Hauser has received monthly notifications from Discover, Experian, and IDNotify, reporting that her PII has been detected on the Dark Web. As a direct and proximate result of the Data Breach, Plaintiff Hauser has experienced an increase in spam/phishing emails and phone calls. As a direct and proximate result of the Data Breach, Plaintiff Hauser spent time, approximately 70 hours, registering for Kroll credit monitoring, researching the Breach, contacting card issuers and/or banks to preemptively get new account numbers issued, and monitoring accounts for suspicious activity. She further expended time contacting Spectrum to assist her in trying to block the phone numbers that have repeatedly spammed her and continue to spam her.

775. Plaintiff Hauser greatly values her privacy and PII and takes reasonable steps to maintain the confidentiality of her PII. Plaintiff Hauser is very careful about sharing her PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Hauser stores any and all documents containing PII in a secure location and destroys any documents she receives in the mail that contain any PII or any information that could otherwise be used to compromise her identity and/or credit. Moreover, Plaintiff Hauser diligently chooses unique usernames and passwords for her various online accounts, and she takes steps to ensure her online accounts are secure and password-protected.

776. Plaintiff Hauser is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud, resulting from the Data Breach. The Data Breach

has caused Plaintiff Hauser to suffer fear, anxiety, and stress, which have been compounded by Progress, PBI, and Genworth's two-month delay in informing her of the fact that her PII, including her Social Security number, was acquired by known cybercriminals through the Data Breach.

777. Plaintiff Hauser anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Hauser will continue to be at present and continued increased risk of identity theft and fraud for years to come.

778. Plaintiff Hauser has a continuing interest in ensuring that her PII, which remains in Progress, PBI, and Genworth's possession, is protected and safeguarded from future disclosure and/or data breaches.

779. Moreover, when Plaintiff Hauser purchased life insurance from Genworth, she did not receive the benefit of the bargain because, had she known that Progress, PBI, and Genworth were using substandard data security policies, she would not have purchased or would have paid less for the Genworth life insurance policy.

780. As a result of the Data Breach, Plaintiff Hauser has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised PII; and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff Hauser now faces a substantial risk that unauthorized third parties will further misuse her PII because (1) the Data Breach involved a single

cybercriminal organization, Cl0p, specifically targeting Defendants' systems; (2) the dataset of PII that Cl0p exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PII Cl0p exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Hauser has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen PII such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time that she spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

781. Plaintiff Hauser experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Hauser would compensate her for the foregoing redressable injuries. Further, Plaintiff Hauser seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of her PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

h. Plaintiff Tricia Hernandez

782. Plaintiff Tricia Hernandez ("Plaintiff Hernandez") is a resident and citizen of the state of Texas and resides in Groves, Texas.

783. Plaintiff Hernandez holds a life insurance policy with GLAIC.

784. Plaintiff Hernandez received a letter directly from Genworth dated July 31, 2023, which reported that "Genworth was recently notified by [PBI] that your personal information was involved in a data security event that took advantage of a vulnerability in the widely used MOVEit file transfer software that PBI uses."

785. Ten days prior, Plaintiff Hernandez received a letter from PBI dated July 21, 2023, which states that PBI "provides audit and address research services for insurance companies, pension funds, and other organizations, including [GLAIC], or for a third party acting on their behalf" and experienced the Data Breach, which "affected the security of some of [Plaintiff Hernandez's] information." The letter states further as follows:

> **What Happened?** On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded your data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.
>
> **What Information Was Involved?** Our investigation determined that the following types of information related to you were present in the server at the time of the event: name, Social Security number, date of birth, zip code, state of residence, role in policy/account (e.g., Annuitant, Joint Insured, Owner, etc.), general product type, and policy/account number.

786. At the time that Progress discovered the data breach—on or around May 31, 2023—Progress, PBI, and Genworth retained Plaintiff Hernandez's PII in their computer systems.

787. Accordingly, the letter states that Progress, PBI, and Genworth possessed Plaintiff Hernandez's PII, including her name, Social Security number, date of birth, zip code, state of residence, role in policy/account (e.g., Annuitant, Joint Insured, Owner, etc.), general product type,

and policy/account number, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

788. According to the letter, Progress, PBI, and Genworth learned of the Data Breach as early as May 29-31, 2023, but they waited approximately two months before they notified Plaintiff Hernandez that her highly sensitive PII was compromised in the Data Breach.

789. In addition to their substantial delay in notifying Plaintiff Hernandez of the Data Breach, Progress, PBI, and Genworth also put the burden on Plaintiff Hernandez to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors . . . and to report suspected identity theft incidents to the insurance company."

790. According to the letter, Progress, PBI, and Genworth waited approximately two months before they notified Plaintiff Hernandez that her PII was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Hernandez, who retains a vested interest in ensuring that her PII remains protected.

791. Moreover, PBI and Genworth's disclosure of the Breach amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Hernandez of the Data Breach's critical facts.

792. Plaintiff Hernandez's PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. As a direct and proximate result of the Data Breach, on August 22, 2023, August 2, 2024, and August 22, 2024, Plaintiff Hernandez received

notifications from IDX identity theft protection, reporting that her PII was detected on the Dark Web. As a direct and proximate result of the Data Breach, Plaintiff Hernandez has experienced an increase in spam/phishing emails, such that she has received thousands of them and continues to receive them daily. As a direct and proximate result of the Data Breach, Plaintiff Hernandez spent time, approximately 425 hours, registering for credit and identity monitoring, assessing phishing emails, researching the Data Breach and monitoring her accounts and credit for suspicious activity.

793. Plaintiff Hernandez greatly values her privacy and PII and takes reasonable steps to maintain the confidentiality of her PII. Plaintiff Hernandez is very careful about sharing her PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Hernandez stores any and all documents containing PII in a secure location and destroys any documents she receives in the mail that contain any PII or any information that could otherwise be used to compromise her identity and/or credit. Moreover, Plaintiff Hernandez diligently chooses unique usernames and passwords for her various online accounts, and she takes steps to ensure her online accounts are secure and password-protected.

794. Plaintiff Hernandez is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud, resulting from the Data Breach. The Data Breach has caused Plaintiff Hernandez to suffer fear, anxiety, anger, rage, physical pain, and stress, which have been compounded by Progress, PBI, and Genworth's two-month delay in informing her of the fact that her PII, including her name and Social Security number, was acquired by known cybercriminals through the Data Breach.

795. Plaintiff Hernandez anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff

Hernandez will continue to be at present and continued increased risk of identity theft and fraud for years to come.

796. Plaintiff Hernandez has a continuing interest in ensuring that her PII, which remains in Progress, PBI, and Genworth's possession, is protected and safeguarded from future disclosure and/or data breaches.

797. Moreover, when Plaintiff Hernandez purchased life insurance from Genworth, she did not receive the benefit of the bargain because, had she known that Progress, PBI, and Genworth were using substandard data security policies, she would not have purchased or would have paid less for the Genworth life insurance policy.

798. As a result of the Data Breach, Plaintiff Hernandez has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised PII; and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff Hernandez now faces a substantial risk that unauthorized third parties will further misuse her PII because (1) the Data Breach involved a single cybercriminal organization, Cl0p, specifically targeting Defendants' systems; (2) the dataset of PII that Cl0p exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PII Cl0p exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other

financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Hernandez has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen PII such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time that she spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

799. Plaintiff Hernandez experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Hernandez would compensate her for the foregoing redressable injuries. Further, Plaintiff Hernandez seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of her PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

i. Plaintiff Rita Pasquarelli

800. Plaintiff Rita Pasquarelli ("Plaintiff Pasquarelli") is a resident and citizen of the state of California, and resides in Temecula, California.

801. Plaintiff Pasquarelli holds a life insurance policy with Genworth.

802. Plaintiff Pasquarelli received a letter from PBI dated July 21, 2023, which states that PBI "provides audit and address research services for insurance companies, pension funds, and other organizations, including [GLAIC], or for a third party acting on their behalf," and experienced the Data Breach, which "affected the security of some of [Plaintiff Pasquarelli's] information." The letter states further as follows:

> **What Happened?** On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.
>
> **What Information Was Involved?** Our investigation determined that the following types of information related to you were present in the server at the time of the event: name, Social Security number, date of birth, zip code, state of residence, role in policy/account (e.g., Annuitant, Joint Insured, Owner, etc.), general product type, and policy/account number.

803. At the time that Progress discovered the data breach—on or around May 31, 2023—Progress, PBI, and Genworth retained Plaintiff Pasquarelli's PII in their computer systems.

804. Accordingly, the letter states that Progress, PBI, and Genworth possessed Plaintiff Pasquarelli's PII, including her name, Social Security number, date of birth, zip code, state of residence, role in policy/account, general product type, and policy/account number, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

805. According to the letter, Progress, PBI, and Genworth learned of the Data Breach as early as May 29-31, 2023, but they waited approximately two months before only PBI notified Plaintiff Pasquarelli that her highly sensitive PII was compromised in the Data Breach.

806. In addition to their substantial delay in notifying Plaintiff Pasquarelli of the Data Breach, Progress, PBI, and Genworth also put the burden on Plaintiff Pasquarelli to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors . . . and to report suspected identity theft incidents to the insurance company."

807. According to the letter, Progress, PBI, and Genworth waited two months before they notified Plaintiff Pasquarelli that her PII was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Pasquarelli, who retains a vested interest in ensuring that her PII remains protected.

808. Moreover, PBI's disclosure of the Breach amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Pasquarelli of the Data Breach's critical facts.

809. Plaintiff Pasquarelli's PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. Plaintiff Pasquarelli encountered an increase in many inappropriate spam/phishing calls, emails, and text messages to her Outlook account. Additionally, in or about August 2023 and September 2023, Plaintiff Pasquarelli received notifications from Experian and CreditWise credit monitoring that her PII was detected on the Dark Web. As a direct and proximate result of the Data Breach, she spent time, approximately 60 hours, researching the Breach, contacting Genworth about the Breach, contacting major credit bureaus to freeze credit, monitoring accounts for suspicious activity, and investigating fraudulent/suspicious activity.

810. Plaintiff Pasquarelli greatly values her privacy and PII and takes reasonable steps to maintain the confidentiality of her PII. Plaintiff Pasquarelli is very careful about sharing her PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Pasquarelli stores any and all documents containing PII in a secure location and destroys any documents she receives in the mail that contain any PII or any information that could otherwise be used to compromise her identity and/or credit. Moreover, Plaintiff Pasquarelli

diligently chooses unique usernames and passwords for her various online accounts, and she takes steps to ensure her online accounts are secure and password-protected.

811. Plaintiff Pasquarelli is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud, resulting from the Data Breach. The Data Breach has caused Plaintiff Pasquarelli to suffer fear, anxiety, sleep disruption, rage, anger, physical pain, and stress, which have been compounded by Progress, PBI, and Genworth's two-month delay in informing her of the fact that her PII, including her Social Security number, was acquired by known cybercriminals through the Data Breach.

812. Plaintiff Pasquarelli anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Pasquarelli will continue to be at present and continued increased risk of identity theft and fraud for years to come.

813. Plaintiff Pasquarelli has a continuing interest in ensuring that her PII, which remains in Progress, PBI, and Genworth's possession, is protected and safeguarded from future disclosure and/or data breaches.

814. As a result of the Data Breach, Plaintiff Pasquarelli has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised PII; and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff Pasquarelli now faces a substantial risk that unauthorized

third parties will further misuse her PII because (1) the Data Breach involved a single cybercriminal organization, Cl0p, specifically targeting Defendants' systems; (2) the dataset of PII that Cl0p exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PII Cl0p exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Pasquarelli has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen PII such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time that she spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

815. Plaintiff Pasquarelli experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Pasquarelli would compensate her for the foregoing redressable injuries. Further, Plaintiff Pasquarelli seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of her PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

2. PBI Bellwether Plaintiff Alleging Claims Against Milliman Defendants and MLIC

a. Plaintiff Jose Soto

816. Plaintiff Jose Soto ("Plaintiff Soto") is a resident and citizen of the state of Florida and resides in Kissimmee, Florida.

817. Plaintiff Soto received a letter from PBI dated July 21, 2023, which states that PBI "provides audit and address research services for insurance companies, pension funds, and other organizations, including MEMBERS Life Insurance Company ("MLIC")," and experienced the Data Breach, which "may affect the security of some of [Plaintiff Soto's] information." The letter states further as follows:

> **What Happened?** On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review on June 16, 2023, and confirmed that information concerning a limited number of MLIC's consumers was among the records involved in this incident.
>
> **What Information Was Involved?** Our investigation determined that the following types of information related to you were present in the server at the time of the event: name, address, date of birth, and Social Security number.

818. At the time that Progress discovered the data breach—on or around May 31, 2023—Progress, PBI, and MLIC retained Plaintiff Soto's PII in their computer systems.

819. Accordingly, the letter states that Progress, PBI, and MLIC possessed Plaintiff Soto's PII, including his name, address, date of birth, and Social Security number, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

820. According to the letter, Progress, PBI, and MLIC learned of the Data Breach as early as May 29-31, 2023, but they waited approximately two months before only PBI notified Plaintiff Soto that his highly sensitive PII was compromised in the Data Breach.

821. In addition to their substantial delay in notifying Plaintiff Soto of the Data Breach, Progress, PBI, and MLIC also put the burden on Plaintiff Soto to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

822. According to the letter, Progress, PBI, and MLIC waited two months before they notified Plaintiff Soto that his PII was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Soto, who retains a vested interest in ensuring that his PII remains protected.

823. Moreover, PBI's disclosure of the Breach amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Soto of the Data Breach's critical facts.

824. As a direct and proximate result of the Data Breach, Plaintiff Soto spent time registering for Kroll credit monitoring. As a direct and proximate result of the Data Breach, he spent time researching the Breach, contacting MLIC about the Breach, contacting major credit bureaus to freeze credit, and contacting banks, credit card companies, or other vendors about fraudulent/suspicious activity.

825. Plaintiff Soto greatly values his privacy and PII and takes reasonable steps to maintain the confidentiality of his PII. Plaintiff Soto is very careful about sharing his PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

Plaintiff Soto stores any and all documents containing PII in a secure location and destroys any documents he receives in the mail that contain any PII or any information that could otherwise be used to compromise his identity and/or credit. Moreover, Plaintiff Soto diligently chooses unique usernames and passwords for his various online accounts, and he takes steps to ensure his online accounts are secure and password-protected.

826. Plaintiff Soto is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud, resulting from the Data Breach. The Data Breach has caused Plaintiff Soto to suffer fear, anxiety, and stress, which have been compounded by Progress, PBI, and MLIC's two-month delay in informing him of the fact that his PII, including his Social Security number, was acquired by known cybercriminals through the Data Breach.

827. Plaintiff Soto anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Soto will continue to be at present and continued increased risk of identity theft and fraud for years to come.

828. Plaintiff Soto has a continuing interest in ensuring that his PII, which remains in Progress, PBI, and MLIC's possession, is protected and safeguarded from future disclosure and/or data breaches.

829. Moreover, when Plaintiff Soto purchased life insurance from MLIC, he did not receive the benefit of the bargain because, had he known that Progress, PBI, and MLIC were using substandard data security policies, he would not have purchased or would have paid less for the MLIC life insurance policy.

830. As a result of the Data Breach, Plaintiff Soto has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the

unauthorized use of his stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of his personal data; lost property in the form of his compromised PII; and injury to his privacy. Additionally, as a direct result of the Data Breach, Plaintiff Soto now faces a substantial risk that unauthorized third parties will further misuse his PII because (1) the Data Breach involved a single cybercriminal organization, Cl0p, specifically targeting Defendants' systems; (2) the dataset of PII that Cl0p exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PII Cl0p exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Soto has (1) suffered, or is at an increased risk of suffering, unauthorized use of his stolen PII such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm because he lost time that he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort he expended addressing future consequences of the Data Breach.

831. Plaintiff Soto experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Soto would compensate him for the foregoing redressable injuries. Further, Plaintiff

Soto seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of his PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

3. PBI Bellwether Plaintiffs Alleging Claims Against TIAA

a. Plaintiff Steven Checchia

832. Plaintiff Steven Checchia ("Plaintiff Checchia") is a resident and citizen of the state of Pennsylvania and resides in Aston, Pennsylvania.

833. Plaintiff Checchia obtained financial services from TIAA and provided his PII to TIAA from his residence in Pennsylvania. He has paid various fees to TIAA for its financial services.

834. Plaintiff Checchia received a letter from PBI dated July 14, 2023, which states that PBI "provides audit and address research services for insurance companies, pension funds, and other organizations, including [TIAA]," and experienced the Data Breach, which "may affect the security of some of [Plaintiff Checchia's] information." The letter states further as follows:

> **What Happened?** On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.
>
> **What Information Was Involved?** Our investigation determined that the following types of information related to you were present in the server at the time of the event: name, Social Security number, gender, date of birth, and address.

835. At the time that Progress discovered the data breach—on or around May 31, 2023—Progress, PBI, and TIAA retained Plaintiff Checchia's PII in their computer systems.

836. Accordingly, the letter states that Progress, PBI, and TIAA possessed Plaintiff Checchia's PII, including his name, Social Security number, gender, date of birth, and address, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

837. According to the letter, Progress, PBI, and TIAA learned of the Data Breach as early as May 29 31, 2023, but they waited approximately two months before only PBI notified Plaintiff Checchia that his highly sensitive PII was compromised in the Data Breach.

838. In addition to their substantial delay in notifying Plaintiff Checchia of the Data Breach, Progress, PBI, and TIAA also put the burden on Plaintiff Checchia to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect."

839. According to the letter, Progress, PBI, and TIAA waited two months before they notified Plaintiff Checchia that his PII was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Checchia, who retains a vested interest in ensuring that his PII remains protected.

840. Moreover, PBI's disclosure of the Breach amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Checchia of the Data Breach's critical facts.

841. Plaintiff Checchia's PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. On or around January to February 2024, Plaintiff Checchia incurred three fraudulent CashApp charges on a Bank of America account. Plaintiff

Checchia called Bank of America and filled out an online form to reverse the charges. On October 9, 2024, Plaintiff Checchia incurred attempted fraudulent CashApp charges on a Chase account. Plaintiff Checchia requested that CashApp stop the payment. On October 10, 2024, Plaintiff Checchia incurred approximately seven fraudulent CashApp charges; four charges were completed, but at least three other charges were attempted. Plaintiff Checchia filled out an online form to dispute the charges; he also cancelled the account and was issued a new card. On October 13, 2024, Plaintiff Checchia received an email from Chase Bank, stating that someone attempted to access his Chase account through multiple computers. Plaintiff Checchia called Chase, cancelled the account, and was issued a new card. On October 14, 2024, Plaintiff Checchia incurred one fraudulent charged on an Image credit card; he cancelled the card and was issued a new one. Also on October 14, 2024, Plaintiff Checchia received a text message from Chase Bank, stating that it declined a transaction on his Chase debit card. Plaintiff Checchia responded to Chase Bank and confirmed that it was an unauthorized and fraudulent transaction. On October 18 and 19, 2024, Plaintiff Checchia received a phone call from MoneyLion stating that an unknown party attempted to secure a loan in Plaintiff Checchia's name, and an email stating that an unknown party signed into Plaintiff Checchia's MoneyLion account. Plaintiff Checchia spoke with MoneyLion, and the loan was blocked. Additionally, Plaintiff Checchia received a notification from Aura credit/identity theft protection, reporting that his PII was detected on the Dark Web. And on November 12, 2024, Plaintiff Checchia received another Dark Web notification from Aura credit/identity theft protection, reporting that his Social Security number was detected on the Dark Web. The Dark Web notification stated that the notification alert was from the "Moveit – Tiaa.org" Data Breach.

842. As a direct and proximate result of the Data Breach, Plaintiff Checchia spent time, approximately twelve hours, registering for Aura credit and identity theft monitoring, researching the Breach, contacting TIAA about the Breach, monitoring his accounts for suspicious activity, investigating fraudulent/suspicious activity, and contacting banks about fraudulent/suspicious activity. Furthermore, Plaintiff Checchia has incurred out-of-pocket expenses as a result of the Data Breach, including paying for Aura credit/identity theft monitoring services.

843. Plaintiff Checchia greatly values his privacy and PII and takes reasonable steps to maintain the confidentiality of his PII. Plaintiff Checchia is very careful about sharing his PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Checchia stores any and all documents containing PII in a secure location and destroys any documents he receives in the mail that contain any PII or any information that could otherwise be used to compromise his identity and/or credit. Moreover, Plaintiff Checchia diligently chooses unique usernames and passwords for his various online accounts, and he takes steps to ensure his online accounts are secure and password-protected.

844. Plaintiff Checchia is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud, resulting from the Data Breach. The Data Breach has caused Plaintiff Checchia to suffer fear, anxiety, rage, anger, physical pain, and stress, which have been compounded by Progress, PBI, and TIAA's two month delay in informing him of the fact that his PII, including his name and Social Security number, was acquired by known cybercriminals through the Data Breach.

845. Plaintiff Checchia anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff

Checchia will continue to be at present and continued increased risk of identity theft and fraud for years to come.

846. Plaintiff Checchia has a continuing interest in ensuring that his PII, which remains in Progress, PBI, and TIAA's possession, is protected and safeguarded from future disclosure and/or data breaches.

847. Moreover, when Plaintiff Checchia obtained financial services from TIAA, he did not receive the benefit of the bargain because, had he known that Progress, PBI, and TIAA were using substandard data security policies, he would not have paid or would have paid less for the TIAA financial services.

848. As a result of the Data Breach, Plaintiff Checchia has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of his stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of his personal data; lost property in the form of his compromised PII; and injury to his privacy. Additionally, as a direct result of the Data Breach, Plaintiff Checchia now faces a substantial risk that unauthorized third parties will further misuse his PII because (1) the Data Breach involved a single cybercriminal organization, Cl0p, specifically targeting Defendants' systems; (2) the dataset of PII that Cl0p exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PII Cl0p exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial

accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Checchia has (1) suffered, or is at an increased risk of suffering, unauthorized use of his stolen PII such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm because he lost time that he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort he expended addressing future consequences of the Data Breach.

849. Plaintiff Checchia experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Checchia would compensate him for the foregoing redressable injuries. Further, Plaintiff Checchia seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of his PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

b. Plaintiff Patricia Marshall

850. Plaintiff Patricia Marshall ("Plaintiff Marshall") is a resident and citizen of the state of Vermont and resides in Burlington, Vermont.

851. Plaintiff Marshall held a retirement account with TIAA. She opened the account, provided her information to TIAA, and paid various fees to TIAA for its financial services from her residence in Vermont.

852. Plaintiff Marshall received a letter from PBI dated August 11, 2023, which states that PBI "provides audit and address research services for insurance companies, pension funds,

and other organizations, including [TIAA]," and experienced the Data Breach, which "may affect the security of some of [Plaintiff Marshall's] information." The letter states further as follows:

> **What Happened?** On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.
>
> **What Information Was Involved?** Our investigation determined that the following types of information related to you were present in the server at the time of the event: name, Social Security number, gender, date of birth, and address.

853. At the time that Progress discovered the data breach—on or around May 31, 2023—Progress, PBI, and TIAA retained Plaintiff Marshall's PII in their computer systems.

854. Accordingly, the letter states that Progress, PBI, and TIAA possessed Plaintiff Marshall's PII, including her name, Social Security number, gender, date of birth, and address, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

855. According to the letter, Progress, PBI, and TIAA learned of the Data Breach as early as May 29-31, 2023, but they waited over two months before only PBI notified Plaintiff Marshall that her highly sensitive PII was compromised in the Data Breach.

856. In addition to their substantial delay in notifying Plaintiff Marshall of the Data Breach, Progress, PBI, and TIAA also put the burden on Plaintiff Marshall to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

857. According to the letter, Progress, PBI, and TIAA waited over two months before they notified Plaintiff Marshall that her PII was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Marshall, who retains a vested interest in ensuring that her PII remains protected.

858. Moreover, PBI's disclosure of the Breach amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Marshall of the Data Breach's critical facts.

859. Plaintiff Marshall's PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. On or around August 2023, Plaintiff Marshall received unknown charges to her North Country Federal Credit Union checking account and her Union Bank checking account. She contacted the banks, and the charges were stopped. On or around October 16, 2024, Plaintiff Marshall encountered an unknown request for money to be sent to an unknown party through her Union Bank account. She contacted the bank to report the fraudulent request, requested a new card, and drove to the bank to pick up the new card. Soon after she received a call from an unknown party alleging to be an employee of the North Country Federal Credit Union bank. She ended the call, and later spoke with a representative of the North Country Federal Credit Union bank, who confirmed that the call was from an unknown party unaffiliated with the North Country Federal Credit Union bank. She requested a new card and drove to the bank to pick up the card. As a direct and proximate result of the Data Breach, she spent time, approximately 40 to 60 hours, researching the Breach, contacting major credit bureaus to freeze credit, contacting card issuers and/or banks to preemptively get new account numbers issued, monitoring accounts for suspicious activity, investigating fraudulent/suspicious activity, and investigating phishing emails, and saving spam emails and voicemails. Furthermore, Plaintiff

Marshall has incurred out-of-pocket expenses as a result of the Data Breach, including taking time off of work to address the fraud and money spent picking up new bank cards.

860. Plaintiff Marshall greatly values her privacy and PII and takes reasonable steps to maintain the confidentiality of her PII. Plaintiff Marshall is very careful about sharing her PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Marshall stores any and all documents containing PII in a secure location and destroys any documents she receives in the mail that contain any PII or any information that could otherwise be used to compromise her identity and/or credit. Moreover, Plaintiff Marshall diligently chooses unique usernames and passwords for her various online accounts, and she takes steps to ensure her online accounts are secure and password-protected.

861. Plaintiff Marshall is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud, resulting from the Data Breach. The Data Breach has caused Plaintiff Marshall to suffer fear, anxiety, anger, sleep disruption, physical pain, and stress, which have been compounded by Progress, PBI, and TIAA's two-month delay in informing her of the fact that her PII, including her Social Security number, was acquired by known cybercriminals through the Data Breach.

862. Plaintiff Marshall anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Marshall will continue to be at present and continued increased risk of identity theft and fraud for years to come.

863. Plaintiff Marshall has a continuing interest in ensuring that her PII, which remains in Progress, PBI, and TIAA's possession, is protected and safeguarded from future disclosure and/or data breaches.

864. Moreover, when Plaintiff Marshall obtained financial services from TIAA, she did not receive the benefit of the bargain because, had she known that Progress, PBI, and TIAA were using substandard data security policies, she would not have paid or would have paid less for the TIAA financial services.

865. As a result of the Data Breach, Plaintiff Marshall has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised PII; and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff Marshall now faces a substantial risk that unauthorized third parties will further misuse her PII because (1) the Data Breach involved a single cybercriminal organization, Cl0p, specifically targeting Defendants' systems; (2) the dataset of PII that Cl0p exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PII Cl0p exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Marshall has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen PII such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time that she spent

taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

866. Plaintiff Marshall experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Marshall would compensate her for the foregoing redressable injuries. Further, Plaintiff Marshall seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of her PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

c. Plaintiff Margaret Phelan

867. Plaintiff Margaret Phelan ("Plaintiff Phelan") is a resident and citizen of the state of New Jersey and resides in Hoboken, New Jersey.

868. Plaintiff Phelan inherited a family member's TIAA account. She provided her PII to TIAA while residing in New Jersey.

869. Plaintiff Phelan received a letter from PBI dated July 14, 2023, which states that PBI "provides audit and address research services for insurance companies, pension funds, and other organizations, including [TIAA]" and experienced the Data Breach, which "may affect the security of some of [Plaintiff Phelan's] information." The letter states further as follows:

> **What Happened?** On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm

> the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.
>
> **What Information Was Involved?** Our investigation determined that the following types of information related to you were present in the server at the time of the event: name, Social Security number, gender, date of birth, and address.

870. At the time that Progress discovered the data breach—on or around May 31, 2023—Progress, PBI, and TIAA retained Plaintiff Phelan's PII in their computer systems.

871. Accordingly, the letter states that Progress, PBI, and TIAA possessed Plaintiff Phelan's PII, including her name, Social Security number, gender, date of birth, and address, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

872. According to the letter, Progress, PBI, and TIAA learned of the Data Breach as early as May 29 31, 2023, but they waited approximately two months before only PBI notified Plaintiff Phelan that her highly sensitive PII was compromised in the Data Breach.

873. In addition to their substantial delay in notifying Plaintiff Phelan of the Data Breach, Progress, PBI, and TIAA also put the burden on Plaintiff Phelan to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

874. According to the letter, Progress, PBI, and TIAA waited approximately two months before they notified Plaintiff Phelan that her PII was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Phelan, who retains a vested interest in ensuring that her PII remains protected.

875. Moreover, PBI's disclosure of the Breach amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Phelan of the Data Breach's critical facts.

876. Plaintiff Phelan's PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. On June 2, 2023, Plaintiff Phelan received a phishing call from an unknown party alleging to be Amazon Security, asserting that people were making fraudulent charges and opening accounts in her name/Social Security number. Because of the phone calls, Plaintiff Phelan made three to four Chase bank wire transfers, using BitCoin (CoinBase), for a total of approximately $215,000.00. As a direct and proximate result of the Data Breach, Plaintiff Phelan spent time, approximately 150 hours, investigating those fraudulent charges, contacting the FBI, Hoboken Police Department, and the FTC to file reports about the phishing call and fraudulent charges, researching the Data Breach, and monitoring her accounts and credit for suspicious activity. Furthermore, Plaintiff Phelan has incurred out-of-pocket expenses as a result of the Data Breach, including fraudulent charges that have not yet been reimbursed in full.

877. Plaintiff Phelan greatly values her privacy and PII and takes reasonable steps to maintain the confidentiality of her PII. Plaintiff Phelan is very careful about sharing her PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Phelan stores any and all documents containing PII in a secure location and destroys any documents she receives in the mail that contain any PII or any information that could otherwise be used to compromise her identity and/or credit. Moreover, Plaintiff Phelan diligently chooses unique usernames and passwords for her various online accounts, and she takes steps to ensure her online accounts are secure and password-protected.

878. Plaintiff Phelan is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud, resulting from the Data Breach. The Data Breach has caused Plaintiff Phelan to suffer fear, anxiety, physical pain, and stress, which have been

compounded by Progress, PBI, and TIAA's two-month delay in informing her of the fact that her PII, including her name and Social Security number, was acquired by known cybercriminals through the Data Breach.

879. Plaintiff Phelan anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Phelan will continue to be at present and continued increased risk of identity theft and fraud for years to come.

880. Plaintiff Phelan has a continuing interest in ensuring that her PII, which remains in Progress, PBI, and TIAA's possession, is protected and safeguarded from future disclosure and/or data breaches.

881. Moreover, when Plaintiff Phelan obtained financial services from TIAA, she did not receive the benefit of the bargain because, had she known that Progress, PBI, and TIAA were using substandard data security policies, she would not have paid or would have paid less for the TIAA financial services.

882. As a result of the Data Breach, Plaintiff Phelan has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised PII; and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff Phelan now faces a substantial risk that unauthorized third parties will further misuse her PII because (1) the Data Breach involved a single

cybercriminal organization, Cl0p, specifically targeting Defendants' systems; (2) the dataset of PII that Cl0p exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PII Cl0p exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Phelan has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen PII such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time that she spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

883. Plaintiff Phelan experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Phelan would compensate her for the foregoing redressable injuries. Further, Plaintiff Phelan seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of her PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

d. Plaintiff Steven Teppler

884. Plaintiff Steven Teppler ("Plaintiff Teppler") is a resident and citizen of the state of Florida and resides in Jacksonville, Florida.

885. Plaintiff Teppler's employer's retirement plan was administered by TIAA. He has paid various fees to TIAA for its financial services.

886. Plaintiff Teppler received a letter from PBI dated July 14, 2023, which states that PBI "provides audit and address research services for insurance companies, pension funds, and other organizations, including [TIAA]," and experienced the Data Breach, which "may affect the security of some of [Plaintiff Teppler's] information." The letter states further as follows:

> **What Happened?** On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.
>
> **What Information Was Involved?** Our investigation determined that the following types of information related to you were present in the server at the time of the event: name, Social Security number, gender, date of birth, and address.

887. At the time that Progress discovered the data breach—on or around May 31, 2023—Progress, PBI, and TIAA retained Plaintiff Teppler's PII in their computer systems.

888. Accordingly, the letter states that Progress, PBI, and TIAA possessed Plaintiff Teppler's PII, including his name, Social Security number, gender, date of birth, and address, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

889. According to the letter, Progress, PBI, and TIAA learned of the Data Breach as early as May 29-31, 2023, but they waited approximately two months before only PBI notified Plaintiff Teppler that his highly sensitive PII was compromised in the Data Breach.

890. In addition to their substantial delay in notifying Plaintiff Teppler of the Data Breach, Progress, PBI, and TIAA also put the burden on Plaintiff Teppler to prevent any further

harm resulting from the Data Breach by stating in the letter: "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors . . . and to report suspected identity theft incidents to the institution."

891. According to the letter, Progress, PBI, and TIAA waited two months before they notified Plaintiff Teppler that his PII was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Teppler, who retains a vested interest in ensuring that his PII remains protected.

892. Moreover, PBI's disclosure of the Breach amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Teppler of the Data Breach's critical facts.

893. Plaintiff Teppler's PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. As a direct and proximate result of the Data Breach, Plaintiff Teppler has encountered an increase in spam/phishing calls, emails, and text messages. Additionally, Plaintiff Teppler received a notification reporting that his PII was detected on the Dark Web. As a direct and proximate result of the Data Breach, Plaintiff Teppler spent time, approximately three to four hours, registering for Experian credit monitoring, researching the Breach, and monitoring accounts for suspicious activity.

894. Plaintiff Teppler greatly values his privacy and PII and takes reasonable steps to maintain the confidentiality of his PII. Plaintiff Teppler is very careful about sharing his PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Teppler stores any and all documents containing PII in a secure location and destroys any documents he receives in the mail that contain any PII or any information that could otherwise be

used to compromise his identity and/or credit. Moreover, Plaintiff Teppler diligently chooses unique usernames and passwords for his various online accounts, and he takes steps to ensure his online accounts are secure and password-protected.

895. Plaintiff Teppler is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud, resulting from the Data Breach. The Data Breach has caused Plaintiff Teppler to suffer fear, anxiety, and stress, which have been compounded by Progress, PBI, and TIAA's two-month delay in informing him of the fact that his PII, including his Social Security number, was acquired by known cybercriminals through the Data Breach.

896. Plaintiff Teppler anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Teppler will continue to be at present and continued increased risk of identity theft and fraud for years to come.

897. Plaintiff Teppler has a continuing interest in ensuring that his PII, which remains in Progress, PBI, and TIAA's possession, is protected and safeguarded from future disclosure and/or data breaches.

898. Moreover, when Plaintiff Teppler's employer obtained financial services from TIAA, he did not receive the benefit of the bargain because, had he known that Progress, PBI, and TIAA were using substandard data security policies, he would not have paid or would have paid less for the TIAA financial services.

899. As a result of the Data Breach, Plaintiff Teppler has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of his stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring his credit and for identity theft; time and expenses spent scrutinizing bank

statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of his personal data; lost property in the form of his compromised PII; and injury to his privacy. Additionally, as a direct result of the Data Breach, Plaintiff Teppler now faces a substantial risk that unauthorized third parties will further misuse his PII because (1) the Data Breach involved a single cybercriminal organization, Cl0p, specifically targeting Defendants' systems; (2) the dataset of PII that Cl0p exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PII Cl0p exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Teppler has (1) suffered, or is at an increased risk of suffering, unauthorized use of his stolen PII such that he has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of his PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by his exposure to the risk of future harm because he lost time that he spent taking protective measures that would have otherwise been put to other productive use and lost opportunity costs associated with the time and effort he expended addressing future consequences of the Data Breach.

900. Plaintiff Teppler experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Teppler would compensate him for the foregoing redressable injuries. Further, Plaintiff Teppler seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of his PII

accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

e. Plaintiff Katharine Uhrich

901. Plaintiff Katharine Uhrich ("Plaintiff Uhrich") is a resident and citizen of the state of Illinois and resides in Forest Park, Illinois.

902. Plaintiff Uhrich used TIAA as a retirement service provider and provided her private information to TIAA while residing in Illinois. She has paid various fees to TIAA for its financial services.

903. Plaintiff Uhrich received a letter from PBI dated July 25, 2023, which states that PBI "provides audit and address research services for insurance companies, pension funds, and other organizations, including [TIAA]" and experienced the Data Breach, which "may affect the security of some of [Plaintiff Uhrich's] information." The letter states further as follows:

> **What Happened?** On or around May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that had been exploited by an unauthorized third party. PBI utilizes MOVEit in the regular course of our business operations to securely transfer files. PBI promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our systems. Through the investigation, we learned that the third party accessed one of our MOVEit Transfer servers on May 29, 2023 and May 30, 2023 and downloaded data. We then conducted a manual review of our records to confirm the identities of individuals potentially affected by this event and their contact information to provide notifications. We recently completed this review.
>
> **What Information Was Involved?** Our investigation determined that the following types of information related to you were present in the server at the time of the event: name, Social Security number, gender, date of birth, and address.

904. At the time that Progress discovered the data breach—on or around May 31, 2023—Progress, PBI, and TIAA retained Plaintiff Uhrich's PII in their computer systems.

905. Accordingly, the letter states that Progress, PBI, and TIAA possessed Plaintiff Uhrich's PII, including her name, Social Security number, gender, date of birth, and address, but failed to protect it and, instead, allowed cybercriminals to access it through the Data Breach.

906. According to the letter, Progress, PBI, and TIAA learned of the Data Breach as early as May 29-31, 2023, but they waited approximately two months before only PBI notified Plaintiff Uhrich that her highly sensitive PII was compromised in the Data Breach.

907. In addition to their substantial delay in notifying Plaintiff Uhrich of the Data Breach, Progress, PBI, and TIAA also put the burden on Plaintiff Uhrich to prevent any further harm resulting from the Data Breach by stating in the letter: "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."

908. According to the letter, Progress, PBI, and TIAA waited two months before they notified Plaintiff Uhrich that her PII was compromised in the Data Breach. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure that such a breach does not occur again have not been explained to Plaintiff Uhrich, who retains a vested interest in ensuring that her PII remains protected.

909. Moreover, PBI's disclosure of the Breach amounts to no real disclosure because it fails to inform, with any degree of specificity, Plaintiff Uhrich of the Data Breach's critical facts.

910. Plaintiff Uhrich's PII compromised in the Data Breach has already been misused by cybercriminals for fraud and identity theft. As a direct and proximate result of the Data Breach, Plaintiff Uhrich encountered an increase in spam/phishing calls. As a direct and proximate result of the Data Breach, she spent time, approximately 40 hours, monitoring accounts for suspicious activity.

911. Plaintiff Uhrich greatly values her privacy and PII and takes reasonable steps to maintain the confidentiality of her PII. Plaintiff Uhrich is very careful about sharing her PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. Plaintiff Uhrich stores any and all documents containing PII in a secure location and destroys any documents she receives in the mail that contain any PII or any information that could otherwise be used to compromise her identity and/or credit. Moreover, Plaintiff Uhrich diligently chooses unique usernames and passwords for her various online accounts, and she takes steps to ensure her online accounts are secure and password-protected.

912. Plaintiff Uhrich is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud, resulting from the Data Breach. The Data Breach has caused Plaintiff Uhrich to suffer fear, anxiety, anger, and stress, which have been compounded by Progress, PBI, and TIAA's two-month delay in informing her of the fact that her PII, including her Social Security number, was acquired by known cybercriminals through the Data Breach.

913. Plaintiff Uhrich anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Uhrich will continue to be at present and continued increased risk of identity theft and fraud for years to come.

914. Plaintiff Uhrich has a continuing interest in ensuring that her PII, which remains in Progress, PBI, and TIAA's possession, is protected and safeguarded from future disclosure and/or data breaches.

915. Moreover, when Plaintiff Uhrich obtained financial services from TIAA, she did not receive the benefit of the bargain because, had she known that Progress, PBI, and TIAA were

using substandard data security policies, she would not have paid or would have paid less for the TIAA financial services.

916. As a result of the Data Breach, Plaintiff Uhrich has already suffered—and is at an increased risk of further suffering—injury and/or damages, including, but not limited to, the unauthorized use of her stolen PII, heightened threat of identity theft and general mitigation efforts spent on monitoring her credit and for identity theft; time and expenses spent scrutinizing bank statements, credit card statements, and credit reports for fraudulent transactions/conduct; time and expenses spent monitoring bank accounts for fraudulent activity; loss in value of her personal data; lost property in the form of her compromised PII; and injury to her privacy. Additionally, as a direct result of the Data Breach, Plaintiff Uhrich now faces a substantial risk that unauthorized third parties will further misuse her PII because (1) the Data Breach involved a single cybercriminal organization, Cl0p, specifically targeting Defendants' systems; (2) the dataset of PII that Cl0p exfiltrated from Defendants' systems has already been actually misused for fraudulent and/or unauthorized conduct; and (3) the type of PII Cl0p exfiltrated in the Data Breach is highly sensitive and can be misused for substantially injurious forms of identity and/or fraud, such as fraudulently applying for and obtaining credit cards, loans, mortgages, bank accounts, or other financial accounts in Plaintiff's name. As a result of the Data Breach, Plaintiff Uhrich has (1) suffered, or is at an increased risk of suffering, unauthorized use of her stolen PII such that she has suffered concrete injury; (2) suffered concrete injury in fact based on the material risk of future misuse of her PII and concrete harm by exposure to this risk; and (3) experienced separate concrete, present harm caused by her exposure to the risk of future harm because she lost time that she spent taking protective measures that would have otherwise been put to other productive use and lost

opportunity costs associated with the time and effort she expended addressing future consequences of the Data Breach.

917. Plaintiff Uhrich experienced all of the foregoing harm and injury as a direct result of Defendants' actions and inactions that led to the Data Breach. The monetary relief sought herein by Plaintiff Uhrich would compensate her for the foregoing redressable injuries. Further, Plaintiff Uhrich seeks injunctive relief to redress the foregoing injuries and harm, including, but not limited to, requiring Defendants to take steps to monitor for, protect, and/or prevent misuse of her PII accessed by cybercriminals in the Data Breach, as well as enact adequate data privacy/security practices.

III. DEFENDANTS

A. Progress

1. Progress Software Corporation

918. Defendant **Progress Software Corporation** is a public corporation organized under the laws of the State of Delaware with its principal place of business located at 15 Wayside Road, Suite 400, Burlington, Massachusetts 01803.

919. Progress produces software for creating and deploying business applications. Founded in 1981 in Burlington, Massachusetts, it has offices in 16 countries, thousands of employees, and revenues of over $500 million.[25]

[25] *SEC Filing Details*, Progress Software Corporation (Nov. 30, 2021, filed Jan. 27, 2022), https://investors.progress.com/sec-filings/sec-filing/10-k/0000876167-22-000038.

920. Originally called Data Language Corporation, the company changed its name to Progress Software in 1987. In 2016, Progress Software re-branded to "Progress" in an effort to "shed any doubts it was not living up to its name."[26]

921. Progress has seen rapid expansion over the past two decades, acquiring eXcelon Corporation for approximately $24 million in 2002,[27] DataDirect Technologies in 2003 for $88 million,[28] Persistence Software in 2004 for $16 million,[29] and at least a dozen other companies for well over $200 million since then.[30]

922. Progress's insatiable appetite for growth also resulted in its 2019 acquisition of Ipswitch, Inc., an IT management vendor known for its MOVEit managed file transfer platform, for $225 million.[31]

---

[26] Justine Hofherr, *After 35 years, Progress Software introduces a new name and vision*, Bulletin Bostin (Nov. 8, 2016), https://www.builtinboston.com/articles/after-35-years-progress-software-introduces-new-name-and-vision.

[27] Scarlet Pruitt, *Progress buys XML toolmaker eXcelon*, Computerworld (Oct. 21, 2002), https://www.computerworld.com/article/1336237/progress-buys-xml-tool-maker-excelon.html.

[28] Brian Fonseca, *Progress Software Acquires DataDirect*, eWeek (Dec. 8, 2003), https://www.eweek.com/database/progress-software-acquires-datadirect/.

[29] Waters Technology Staff, *Progress to Acquire Persistence for $16M*, WatersTechnology (Oct. 4, 2004), https://www.waterstechnology.com/sell-side-technology/news/1632464/progress-acquire-persistence-usd16m.

[30] *See, e.g.*, Andrew Phelan, *Trinity boys sell college firm for $162m*, Irish Independent (June 26, 2008), https://www.independent.ie/regionals/herald/trinity-boys-sell-college-firm-for-162m/27876930.html; Darryl K. Taft, *Progress Software Acquires Iona*, eWeek (June 25, 2008), https://www.eweek.com/development/progress-software-acquires-iona/; *Progress Software acquires algorithmic technology vendor Apama*, Finextra (Apr. 7, 2005), https://www.finextra.com/newsarticle/13477/progress-software-acquires-algorithmic-technology-vendor-apama; Yogesh Gupta, *Progress to Acquire NoSQL Database Pioneer, MarkLogic*, Progress Blogs (Jan. 3, 2023), https://www.progress.com/blogs/progress-to-acquire-nosql-database-pioneer-marklogic.

[31] Larry Dignan, *Progress acquires Ipswitch for $225 million, tops first quarter targets*, ZDNet (Mar. 28, 2019), https://www.zdnet.com/article/progress-acquires-ipswitch-for-225-million-tops-first-quarter-targets/; *Progress Completes Acquisition of Ipswitch, Inc.*, Progress: Press Release

2. Ipswitch, Inc.

923. Defendant Ipswitch is a wholly-owned subsidiary of Progress with its principal place of business in Burlington, Massachusetts.

924. Founded in 1991, Ipswitch is "a provider of award-winning and easy-to-use secure data file transfer and network management software,"[32] including MOVEit file-transfer software.

925. At the time of its acquisition by Progress, Ipswitch had about $75 million in revenue, approximately 51% of which came from its data file transfer business segment.[33] The company had a global presence with approximately 24,000 active customers in 170 countries.[34]

926. Progress touted its acquisition of Ipswitch as a way to "bolster . . . core offerings for small and medium-sized businesses . . . and enterprises."[35] Approximately ninety Ipswitch employees joined Progress as part of the 2019 acquisition.[36]

B. PBI Bellwether Defendants

1. Pension Benefit Information, LLC

927. Defendant **Pension Benefit Information, LLC**, d/b/a PBI Research Services ("PBI") is a for-profit Delaware corporation with its principal place of business in Minneapolis,

---

(May 1, 2019), https://investors.progress.com/news-releases/news-release-details/progress-completes-acquisition-ipswitch-inc#.

[32] *Progress Completes Acquisition of Ipswitch, Inc.*, Progress: Press Release (May 1, 2019), https://investors.progress.com/news-releases/news-release-details/progress-completes-acquisition-ipswitch-inc#.

[33] Larry Dignan, *Progress acquires Ipswitch for $225 million, tops first quarter targets*, ZDNet (Mar. 28, 2019), https://www.zdnet.com/article/progress-acquires-ipswitch-for-225-million-tops-first-quarter-targets/

[34] *Id.*

[35] *Progress Completes Acquisition of Ipswitch, Inc.*, Progress: Press Release (May 1, 2019), https://investors.progress.com/news-releases/news-release-details/progress-completes-acquisition-ipswitch-inc#.

[36] *Id.*

Minnesota. PBI uses Progress's MOVEit service in the regular course of its business acting as a pension plan "sponsor, administrator, or record keeper" "for thousands of organizations" and pension plans.

2. Genworth Financial, Inc.

928. Defendant **Genworth Financial** is a publicly traded Fortune 500 company Delaware corporation with its principal place of business in Richmond, Virginia. Genworth Financial markets mortgage, long-term care insurance, life insurance, and other insurance and financial products, primarily to individual consumers.

3. Genworth Life and Annuity Insurance Co.

929. Defendant **GLAIC** is a subsidiary of Genworth Financial with its principal place of business in Richmond, Virginia.

4. Genworth Life Insurance Co.

930. Defendant **GLIC** is a subsidiary of Genworth Financial with its principal place of business in Richmond, Virginia.

5. Milliman, Inc. (d/b/a Milliman Intelliscript Inc.)

931. Defendant **Milliman, Inc.** is a Washington corporation with its principal place of business in Seattle, Washington. Milliman provides administrative services to employee benefit and pension plan sponsors.

6. Milliman Solutions, LLC

932. Defendant **Milliman Solutions** is a subsidiary of Milliman, Inc. with its principal place of business in Seattle, Washington. Milliman Solutions markets its business as providing risk assessment services to clients, including life insurance companies.

7. MEMBERS Life Insurance Company

933. Defendant **MLIC** is an Iowa corporation with its principal place of business in Madison, Wisconsin.

8. Teachers Insurance and Annuity Association of America

934. Defendant **TIAA** is a New York based stock insurance company with its principal place of business in New York, New York. TIAA provides services to over 5 million clients from more than 15,000 institutions and manages nearly $1 trillion in assets with holdings in more than 50 countries.

C. Maximus Bellwether Defendants

1. Maximus, Inc.

935. Defendant **Maximus Inc.** is a Virginia corporation and maintains its headquarters and principal place of business at 1600 Tysons Boulevard, McLean, Virginia 22102. Defendant Maximus, Inc. is the parent corporation of Defendant Maximus Federal Services, Inc., Defendant Maximus Health Services, Inc., and Defendant Maximus Human Services, Inc. Defendant Maximus, Inc. acts as a contractor for various State agencies and departments and saves data (including PHI and PII) provided by those agencies in its MOVEit application.

2. Maximus Federal Services, Inc.

936. Defendant **Maximus Federal Services, Inc.** is a Virginia corporation and maintains its headquarters and principal place of business at 1600 Tysons Boulevard, McLean, Virginia 22102. Defendant Maximus Federal Services, Inc. is a wholly owned subsidiary of Maximus, Inc. Defendant Maximus Federal Services, Inc. is a contractor for the Centers for Medicare & Medicaid Services (CMS), and saves data (including PHI and PII) provided by those agencies in its MOVEit application.

3. Maximus Health Services, Inc.

937. Defendant **Maximus Health Services, Inc.** is a "Former Name" for Maximus US Services, Inc., which is an Indiana corporation that maintains its headquarters and principal place of business at 1600 Tysons Boulevard, McLean, Virginia 22102. Defendant Maximus Health Services, Inc. is a wholly owned subsidiary of Maximus, Inc. Defendant Maximus Health Services, Inc. is a contractor to various State agencies and departments and saves data (including PHI and PII) provided by those agencies in its MOVEit application.

4. Maximus Human Services, Inc.

938. Defendant **Maximus Human Services, Inc.** is a Virginia corporation and maintains its headquarters and principal place of business at 1600 Tysons Boulevard, McLean, Virginia 22102. Defendant Maximus Human Services, Inc. is a wholly owned subsidiary of Maximus, Inc. Defendant Maximus Human Services, Inc. is a contractor to various State agencies and departments and saves data (including PII) provided by those agencies in its MOVEit application.

D. Welltok Bellwether Defendants

1. Welltok, Inc.

939. Defendant **Welltok, Inc.** ("Welltok") is a software-as-a-service ("Saas") patient engagement company organized under the laws of Delaware with its principal place of business located at 75 Fountain Street, Suite 310, Providence, Rhode Island 02902. Prior to being acquired by Virgin Pulse in November 2021, Welltok's principal place of business was located at 1515 Arapahoe Street, Tower 3 – Suite 700, Denver, Colorado 80202. Since November 2021, Welltok has been a subsidiary of Virgin Pulse.

940. Welltok is a data-driven patient engagement company that utilizes a single platform to connect healthcare providers with patients by providing personalized, consumer-facing

healthcare content and technology, including patient-communications services. By delivering personalized resources to individuals, Welltok's platform helps individuals take critical actions such as scheduling a doctor's appointment, selecting insurance coverage, or refilling medications. Welltok's platform maintains a massive consumer database that stores and transfers the Private Information of its healthcare patients, clients, and employees using the MOVEit Transfer tool.

941. More than 100 healthcare providers, health plans, employers, and pharmacies contracted with Welltok as a vendor to run patient engagement and acquisition campaigns and store their patients' Private Information on Welltok's platform, including Defendants Baylor Scott, Corewell Health, Sutter Health, OSF, CHI, and Virginia Mason (collectively, "Welltok VCE Defendants"), as well as the following other clients (collectively, "Welltok Clients"):

- Aetna
- Adventist Healthcare
- Altru
- Asuris Northwest Health
- Anthem Blue Cross and Blue Shield
- Arkansas Blue Cross and Blue Shield
- Baxter International Inc. and Subsidiaries Welfare Benefit Plan
- Baylor Scott & White Health
- BridgeSpan Health
- Blue Cross and Blue Shield of Massachusetts
- Blue Cross and Blue Shield of Minnesota and Blue Plus
- Blue Cross and Blue Shield of Alabama
- Blue Cross and Blue Shield of Kansas
- Blue Cross and Blue Shield of North Carolina
- Blue Cross Blue Shield of Illinois
- Blue Cross Blue Shield of Texas
- Blue Cross Blue Shield of New Mexico
- Blue Cross Blue Shield of Oklahoma
- Blue Cross Blue Shield of Montana
- Blue Cross Blue Shield of Massachusetts.
- Blue Cross and Blue Shield of Kansas
- Blue Cross and Blue Shield of Kansas City
- Blue Cross of Idaho Health Service, Inc.
- Blue Cross Blue Shield of Massachusetts
- BlueCross & BlueShield of Minnesota

- Blue Cross & Blue Shield of Mississippi, A Mutual Insurance Company
- Blue Cross and Blue Shield of North Carolina
- Blue Cross Blue Shield of North Dakota
- Blue Cross and Blue Shield of Nebraska
- Blue Cross & Blue Shield of Rhode Island
- Blue Cross Blue Shield of South Carolina
- BlueCross BlueShield of Tennessee
- Blue Cross and Blue Shield of Vermont
- Blue Cross Blue Shield of Wyoming
- Blue Cross and Blue Shield of Arizona, Inc.
- Blue Shield of California
- Blue Shield of California OR Blue Shield of California Promise Health Plan
- Capital Blue Cross
- CareFirst of Maryland, Inc. dba CareFirst BlueCross BlueShield
- Centerwell Pharmacy
- CHI Memorial – TN
- CHI Memorial – GA
- CHI Mercy Health
- CHI St. Joseph Health
- CHI St. Luke's Health Brazosport
- CHI St. Luke's Health Memorial
- CHI St. Vincent
- Community Health Network
- Community Health Group
- Ella EM Brown Charitable Circle dba Oaklawn Hospital
- EmblemHealth Plan, Inc.
- EmblemHealth Insurance Company
- Evoqua Water Technologies
- Excellus Health Plan, Inc.
- Faith Regional Health Services
- Florida Blue
- Freedom Health, Inc.
- Group Hospitalization and Medical Services Inc., dba CareFirst BlueCross BlueShield
- Hawaii Medical Service Association
- Health First Shared Services, Inc
- Health Insurance Plan of Greater New York
- Highmark Inc.,
- Highmark Inc.
- Highmark Western and Northeastern New York
- Highmark Delaware
- Highmark West Virginia
- Highmark Blue Cross Blue Shield Delaware
- Highmark Blue Cross Blue Shield West Virginia

- Highmark Blue Cross Blue Shield of Western New York
- Highmark Blue Shield Northeastern New York
- Holzer Health System
- Horizon Blue Cross Blue Shield of New Jersey
- Hospital & Medical Foundation of Paris, Inc. dba Horizon Health
- Humana Inc.
- Independence Blue Cross
- Johns Hopkins Health Plans
- Louisiana Health Service & Indemnity Company d/b/a Blue Cross and Blue Shield of Louisiana
- Marshfield Clinic Health System
- Mass General Brigham Health Plan
- MetroPlus Health Plan
- Mercy Med Ctr Des Moines-IA
- MercyOne Newton Med Ctr-IA (Skiff)
- Mercy Med Ctr W Lakes Des Moines-IA
- Mercy Med Ctr Centerville-IA
- MercyOne IA Heart Des Moines-IA
- Optum Specialty Pharmacy
- Optum OrthoNet
- Optum AppleCare Medical Group
- Optimum HealthCare, Inc.
- Pinellas County Sherriff's Office
- Premier Health
- Priority Health
- Premera Blue Cross
- Regence BlueCross BlueShield of Oregon
- Regence BlueShield
- Regence BlueCross BlueShield of Utah
- Regence Blue Shield of Idaho
- St. Alexius Health
- St Anthony Hospital
- St. Bernards Healthcare
- St Joseph Health
- St. Luke's Health
- ThedaCare, Inc.
- Taylor Farms
- United Regional Health Care System
- United Healthcare Services, Inc.
- Trane Technologies Company LLC and/or group health plans sponsored by Trane Technologies Company LLC or Trane U.S. Inc.
- Triple-S Salud, Inc.
- Trinity Health System

- The group health plans of Stanford Health Care, of Stanford Health Care, Lucile Packard Children's Hospital Stanford, Stanford Health Care Tri-Valley, Stanford Medicine Partners, and Packard Children's Health Alliance
- The Guthrie Clinic
- West Virginia University Health System
- Wellmark Advantage: Blue Cross Blue Shield Of Michigan
- Wellmark, Inc., d/b/a Wellmark Blue Cross and Blue Shield of Iowa, and Wellmark of South Dakota, Inc. d/b/a Wellmark Blue Cross and Blue Shield of South Dakota
- Wipro Medical
- Yale New Haven Health

942. On November 10, 2021, Virgin Pulse, Inc., a software development company with its principal place of business also located at 75 Fountain Street, Providence, Rhode Island 02902, issued a press release, announcing that it had completed its acquisition of Welltok, which stated that "[c]ombining Welltok's activation engine with Virgin Pulse's daily engagement platform will drive better health outcomes and cost reductions for the companies' 4,100 global employer, health plan and health system clients." According to Virgin Pulse, "[w]ith this acquisition, Virgin Pulse will introduce the industry's first end-to-end engagement and activation platform that supports clients, members, and consumers across the entire health continuum by," among other things, "[l]everaging the industry's most comprehensive consumer database for 275 million lives."

943. On or around February 7, 2024, Virgin Pulse and HealthComp, a third-party administrator for health benefits, rebranded itself under a new company brand called Personify Health, which, like Welltok, maintains headquarters at 75 Fountain Street, Providence, Rhode Island 02902.

2. Corewell Health

944. Defendant **Corewell Health East** ("Corewell" or "Corewell Health") is a Michigan non-profit healthcare corporation that is based in the State of Michigan, headquartered at 100 Michigan St. NE, Grand Rapids, MI 49503 and operating within three designated regions of

Michigan: Southeast Michigan (formerly known as Beaumont Health), Southwest Michigan (formerly known as Spectrum Health Lakeland), and West Michigan (formerly known as Spectrum Health). On October 11, 2022, Beaumont Health and Spectrum Health merged and named the newly formed entity Corewell Health.

3. Sutter Health

945. Defendant **Sutter Health** is a California non-profit corporation, with its principal place of business located at 2710 Gateway Oaks Drive, Sacramento, California 95833. It was created through the January 1996 merger of the Sacramento-based Sutter Health and the Bay Area-based California Healthcare System.

4. OSF Healthcare System

946. Defendant **OSF Healthcare System** ("OSF") is an Illinois not-for-profit corporation headquartered at 124 SW Adams Street Peoria, Illinois 61602 that operates a medical group, hospital system, and other health care facilities in Illinois and Michigan.

5. CHI Health – NE

947. Defendant **CHI Health - NE** ("CHI") is a non-profit, Catholic healthcare system created in February 2019. The CHI network includes approximately 28 acute care hospitals, 18 critical access hospitals, 200 clinic locations, and 4,122 employed physicians providing healthcare services to communities in Nebraska, Southwest Iowa, Minnesota, and North Dakota. CHI is headquartered at 12809 W Dodge Rd, Omaha, Nebraska, 68154.

948. CHI is a member of CommonSpirit Health, a large health system including Catholic Health Initiatives providers and Dignity Health providers across 21 states. All members of CommonSpirit Health participate in an Organized Health Care Arrangement (the CommonSpirit Health OHCA), so they can share health information within CommonSpirit Health for treatment, payment, and joint health care operations activities. Those joint operations activities may include

quality improvement, risk management, financial and billing services, and health information exchanges.

6. Virgnia Mason Franciscan Health

949. Defendant **Virginia Mason Franciscan Health** ("Virginia Mason") is an integrated hospital, training and research facility with hospitals, clinics and outpatient centers, providing health care services to patients throughout the Pacific Northwest and Puget Sound Area in the state of Washington. Virginia Mason is a Washington nonprofit corporation and is headquartered at 1145 Broadway Plaza, Tacoma, WA 98402.

950. Like Defendant CHI, Defendant Virginia Mason is a member of CommonSpirit Health, a large health system including Catholic Health Initiatives providers and Dignity Health providers across 21 states. Virginia Mason's Notice of Privacy Practices includes "Franciscan Medical Group, Center for Integrative Medicine at Virginia Mason, P.C. and Benaroya Research Institute at Virginia Mason. All members of CommonSpirit Health participate in an Organized Health Care Arrangement (the CommonSpirit Health OHCA), so that they can share health information within CommonSpirit Health for treatment, payment, and joint health care operations activities."

7. Baylor Scott & White Health

951. Defendant **Baylor Scott & White Health** ("Baylor Scott") is a Texas non-profit corporation, headquartered at 301 N. Washington Ave., Dallas, TX 75246. Formed in 2013 from the merger of Scott & White Health with Baylor Healthcare System, Baylor Health has become the largest non-profit healthcare system in Texas and one of the largest in the country, consisting of 51 hospitals, more than 800 patient care sites, more than 7,300 active physicians, over 49,000 employees, and the Scott & White Health Plan.

E. Delta Dental Bellwether Defendants

1. Delta Dental of California

952. Defendant **Delta Dental of California** ("DDCA") is a nonprofit 501(c)(4) corporation, incorporated in California, that operates as a dental insurance provider in California. Its principal place of business is located at 560 Mission Street, #1300, San Francisco, California, 94105. The Delta Dental of California enterprise includes various affiliates, including Delta Dental Insurance Company, Delta Dental of Pennsylvania, Delta Dental of New York, Inc., and their affiliated companies, as well as the national DeltaCare USA network. Collectively, these affiliates are referred to as "Delta Dental of California and Affiliates."

2. Delta Dental Insurance Company

953. **Delta Dental Insurance Company** ("DDIC") an affiliate of "Delta Dental of California and Affiliates," operates and administers insurance plans in Alabama, Florida, Georgia, Louisiana, Mississippi, Montana, Nevada, Utah, and Texas. It is headquartered in California at 560 Mission Street, #1300, San Francisco, CA, 94105.

3. Delta Dental of New York

954. Defendant **Delta Dental of New York**, an affiliate of "Delta Dental of California and Affiliates," is a nonprofit 501(c)(4) corporation that operates and administers dental insurance plans in New York. It is headquartered in California at 560 Mission Street, #1300, San Francisco, CA, 94105.

4. Delta Dental of Pennsylvania

955. **Delta Dental of Pennsylvania**, an affiliate of "Delta Dental of California and Affiliates," is a nonprofit 501(c)(4) corporation that operates and administers dental insurance plans in Pennsylvania and Maryland. It is headquartered in California at 560 Mission Street, #1300, San Francisco, CA, 94105.

5. Delta Dental Plans Association

956. **Delta Dental Plans Association** is an Illinois 501(c)(6) not-for-profit national network of Delta Dental Companies, headquartered at 1515 W 22nd St # 450, Oak Brook, Illinois 60523.

957. Other Defendants have also been named as part of the above-captioned multidistrict litigation; however, they are not included as part of the bellwether process of this MDL.

JURISDICTION AND VENUE

958. This Consolidated Amended Complaint is a "bellwether" complaint filed pursuant to the Court's November 6, 2024 Order. ECF No. 1275. It is intended to be the operative pleading against the Defendants, as defined herein.

959. This Court has subject-matter jurisdiction pursuant to Article III of the United States Constitution, as the actions of certain Plaintiffs were removed by certain Defendants to federal courts, which were then centralized as part of this MDL. The Court's subject-matter jurisdiction exists pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, and Defendants are citizens of States different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

960. Absent the Court's MDL Order No. 12 (Direct Filing Order), PBI Bellwether Plaintiffs Brinitha Harris and Rita Pasquarelli would have otherwise filed their cases in the United States District Court for the District of Minnesota, which has personal jurisdiction over PBI Bellwether Plaintiffs' claims against PBI Bellwether Defendants because PBI Bellwether Defendants and their affiliates conduct business in the State of Minnesota that establish sufficient minimum contacts with the District of Minnesota and committed acts therein that give rise to PBI

Bellwether Plaintiffs' claims in this action—including, but not limited to, transferring, storing, or otherwise maintaining PBI Bellwether Plaintiffs' PII in Minnesota and/or engaging in conduct or failing to take steps in Minnesota to prevent the Data Breach, such that the exercise of jurisdiction over PBI Bellwether Defendants would not offend traditional notions of fair play and substantial justice. The District of Minnesota is the proper venue for PBI Bellwether Plaintiffs' claims pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to PBI Bellwether Plaintiffs' claims occurred in that District and PBI Bellwether Defendants have harmed PBI Bellwether Class Members residing in that District.

961. Venue is proper in this District for pretrial purposes as the Judicial Panel on Multidistrict Litigation determined that "centralization of these actions in the District of Massachusetts will serve the convenience of the parties and witnesses and promote the just and efficient conduct of the litigation." *In re MOVEit Customer Data Sec. Breach Litig.*, 699 F. Supp. 3d 1402, 1405 (J.P.M.L. 2023).

CHAPTER ONE:

FACTUAL ALLEGATIONS CONCERNING ALL DEFENDANTS

962. Chapter One supplements the Omnibus Common Allegations (ECF 908), which are herein incorporated by reference.

I. The MOVEit Software.

A. MOVEit software and its use by various Defendants.

963. MOVEit is a file transfer program used by a wide range of organizations in the public and private sector to move highly sensitive consumer data.

964. Financial services companies, government agencies, pension funds, hospitals, universities, banks, health systems, energy and technology companies, and a wide variety of other institutions use the MOVEit product.

965. MOVEit is offered in both on-premises—MOVEit Transfer—and cloud-based—MOVEit Cloud—versions.

1. MOVEit Transfer.

966. Standard Networks, Inc. first developed and released the MOVEit family of software in February 2002 to allow customers to securely transfer files over the Internet.[37] Standard Networks, Inc. was acquired by Ipswitch, Inc.,[38] which was then acquired by Progress in 2019.[39]

---

[37] *Standard Networks releases secure transfer client*, WTN News (Mar. 24, 2004), http://wtnnews.com/articles/700/ [https://web.archive.org/web/20110807192045/http://wtnnews.com/articles/700/].

[38] *Standard Networks acquired by Ipswitch*, Milwaukee Bus. J. (Feb. 19, 2008), https://www.bizjournals.com/milwaukee/stories/2008/02/18/daily8.html.

[39] Larry Dignan, *Progress acquires Ipswitch for $225 million, tops first quarter targets*, ZDNet (Mar. 28, 2019), https://www.zdnet.com/article/progress-acquires-ipswitch-for-225-million-tops-first-quarter-targets/

967. MOVEit Transfer is software that is licensed to customers on a subscription basis and installed by customers on their own servers.[40]

968. MOVEit Transfer is an "on-premises solution" that allows users to have complete control over business-critical file transfers by consolidating them in one system on their own premises.[41]

969. One of MOVEit Transfer's selling points was its use of SSL/TLS to securely transfer files as well as AES for encrypted storage of files (both described in further detail below), thus ensuring that files can only be read if the user has the appropriate encryption keys, even if the files are stolen.[42]

970. SSL, standing for "Secure Sockets Layer," is an encryption protocol developed in 1995 to communicate securely and privately over the Internet. SSL is the predecessor to TLS, developed in 1999 and standing for Transport Layer Security, which is the standard today. TLS uses a combination of public and private keys to encrypt and decrypt data that is passed over a network, such as the Internet. Use of TLS by a website is denoted by "https," as opposed to "http," in the website address.[43] TLS is virtually unbreakable with existing technology.[44]

971. AES, standing for "Advanced Encryption Standard," is the standard for encryption of electronic data adopted by the United States government since 2001. AES uses a private key to

---

[40] *More Secure Managed File Transfer Software for the Enterprise*, Progress: MOVEit, https://www.progress.com/moveit/moveit-transfer (last visited Nov. 26, 2024).

[41] *Id*.

[42] *Id*.

[43] *What is SSL? | SSL definition*, Cloudflare, https://www.cloudflare.com/learning/ssl/what-is-ssl/ (last visited Nov. 26, 2024).

[44] Dionisie Gitlan, *Cracking SSL Encryption is Out of Human Reach*, SSL Dragon (Apr. 15, 2024), https://www.ssldragon.com/blog/cracking-ssl/.

both encrypt and decrypt data.[45] AES is widely adopted and used around the world by governments, businesses, and software.[46] AES is virtually unbreakable with existing technology.[47]

972. Pursuant to the MOVEit Transfer end user license agreement, Progress provides "bug fixes, patches, upgrades, enhancements, new releases [and] technical support" to customers.[48]

973. MOVEit Transfer's customers are primarily businesses, organizations, and governmental entities. Customers install MOVEit Transfer on their servers, and then users—such as the customer's employees—access the software through a MOVEit Transfer software client installed on a computer, phone, or a website accessible over the Internet that connects to the customer's MOVEit Transfer server.[49]

974. Below are examples of the MOVEit Transfer user interface[50]:

[45] Nat'l Inst. of Standards & Tech., *Advanced Encryption Standard (AES)*, Fed. Info. Processing Standards Publ'n 197-upd1 (May 9, 2023), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf.

[46] Rahul Awati et al., *What is the Advanced Encryption Standard (AES)?*, TechTarget (Feb. 2004), https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard.

[47] Victor Kananda, *Why You Should Use AES 256 Encryption to Secure Your Data*, Progress: Blogs (June 22, 2022), https://www.progress.com/blogs/use-aes-256-encryption-secure-data.

[48] *MOVEit and WS_FTP End User License Agreement*, Progress: Legal Info. (Nov. 2023), https://www.progress.com/legal/license-agreements/moveit-ws-ftp.

[49] *Introduction, MOVEit Transfer 2023.1 Adm'r Guide*, Progress: Prod. Documentation (Apr. 21, 2022), https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/Introduction.html; *Client Access, MOVEit Transfer 2023.1 Adm'r Guide*, Progress: Prod. Documentation (Apr. 6, 2022), https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/Client-Access.html.

[50] *Id*.

Figure 1

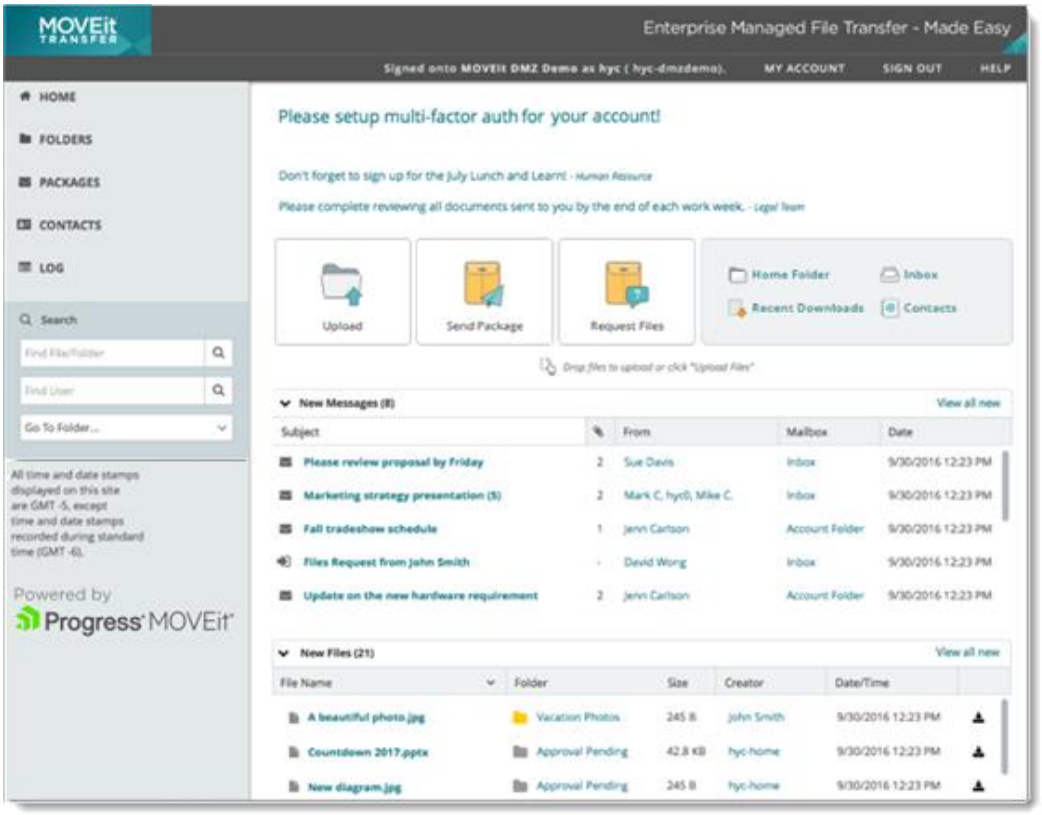
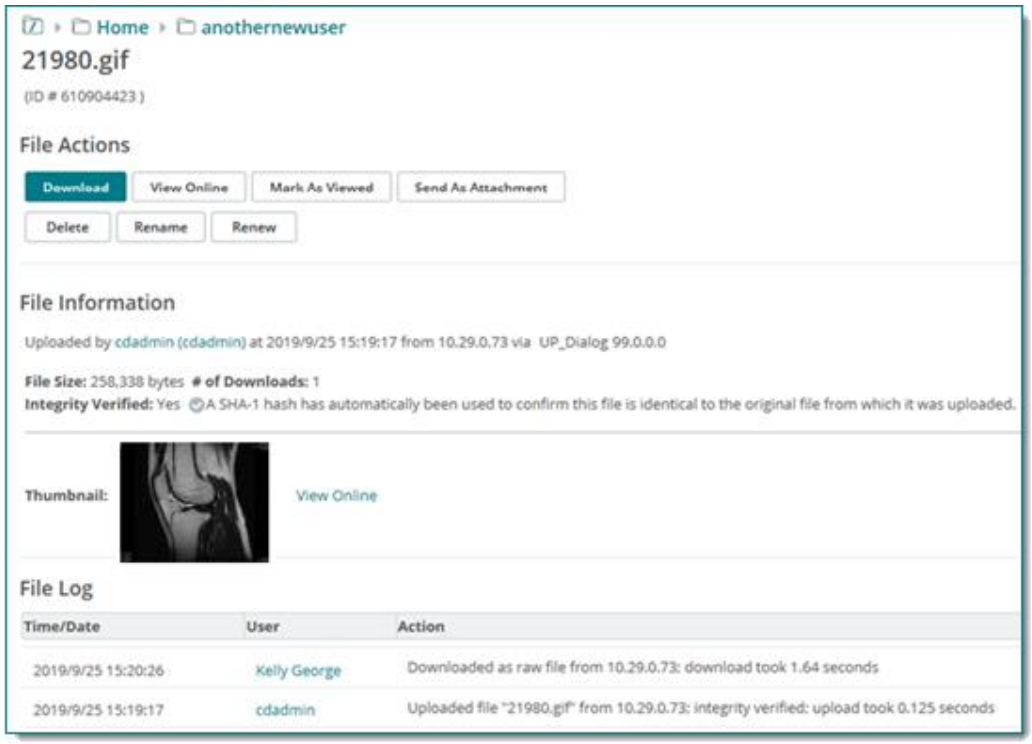

MOVEit TRANSFER
Enterprise Managed File Transfer - Made Easy
Signed onto MOVEit DMZ Demo as hyc (hyc-dmzdemo).
MY ACCOUNT
SIGN OUT
HELP
HOME
FOLDERS
PACKAGES
CONTACTS
LOG
Search
Go To Folder...
All time and date stamps displayed on this site are GMT -5, except time and date stamps recorded during standard time (GMT -6).
Powered by Progress MOVEit
Please setup multi-factor auth for your account!
Don't forget to sign up for the July Lunch and Learn! - Human Resource
Please complete reviewing all documents sent to you by the end of each work week. - Legal Team
Upload
Send Package
Request Files
Home Folder
Inbox
Recent Downloads
Contacts
Drop files to upload or click "Upload Files"
New Messages (8)
View all new
Subject
From
Mailbox
Date
Please review proposal by Friday
Sue Davis
Inbox
9/30/2016 12:23 PM
Marketing strategy presentation (5)
Mark C, hyc0, Mike C.
Inbox
9/30/2016 12:23 PM
Fall tradeshow schedule
Jenn Carlson
Account Folder
9/30/2016 12:23 PM
Files Request from John Smith
David Wong
Inbox
9/30/2016 12:23 PM
Update on the new hardware requirement
Jenn Carlson
Account Folder
9/30/2016 12:23 PM
New Files (21)
View all new
File Name
Folder
Size
Creator
Date/Time
A beautiful photo.jpg
Vacation Photos
245 B
John Smith
9/30/2016 12:23 PM
Countdown 2017.pptx
Approval Pending
42.8 KB
hyc-home
9/30/2016 12:23 PM
New diagram.jpg
Approval Pending
245 B
hyc-home
9/30/2016 12:23 PM

Figure 2



975. Users can also access MOVEit Transfer through a REST API, a programmatic means of interacting with the MOVEit Transfer server without using a graphical user interface such as a client or website.[51]

976. Because the MOVEit Transfer software is installed on customers' public-facing Internet servers, not Progress's servers, the software is accessible by accessing the customers' public website—for example, through *http://moveit.customer-domain-name.com*—not Progress's website.[52]

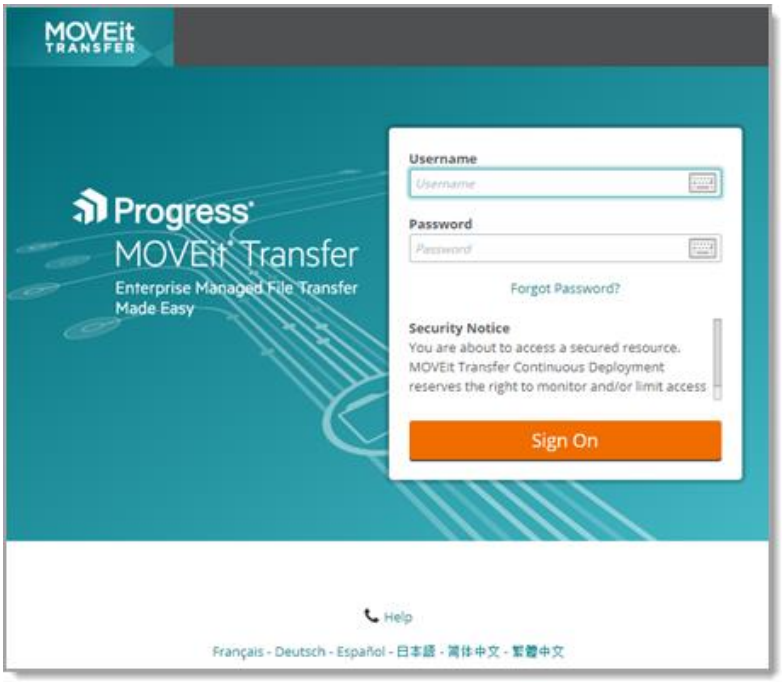
[51] *Id.*

[52] *Advanced Topics: Systems Internal – URL Crafting, MOVEit Transfer 2023.1 Adm'r Guide*, Progress: Prod. Documentation (Apr. 21, 2022), https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/System-Internals-URL-Crafting.html.

977. Authorized users must log into the MOVEit Transfer server with a username and password.[53]

978. Below is a default user login page that would be accessible from a MOVEit Transfer customer's public-facing website on the Internet[54]:

Figure 3



979. After authenticating, users can then transfer files to the MOVEit Transfer server by uploading or downloading files through the MOVEit Transfer client or web application.[55]

[53] *User Guide Welcome: Sign-on, MOVEit Transfer 2023.1 Adm'r Guide*, Progress: Prod. Documentation (Aug. 4, 2022), https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/Sign-On.html.

[54] *Advanced Topics: Systems Internal – URL Crafting, MOVEit Transfer 2023.1 Adm'r Guide*, Progress: Prod. Documentation (Apr. 21, 2022), https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/System-Internals-URL-Crafting.html.

[55] [55] *Introduction, MOVEit Transfer 2023.1 Adm'r Guide*, Progress: Prod. Documentation (Apr. 21, 2022), https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/Introduction.html.

980. Progress claims MOVEit Transfer encrypts files both in transit and at rest so they cannot be viewed at any time without the appropriate encryption key.[56]

2. MOVEit Cloud.

981. Ipswitch developed MOVEit Cloud in 2012.[57]

982. MOVEit Cloud enables the consolidation of all file transfer activities into a cloud-based, online service using Microsoft Azure Cloud servers managed by Progress.[58]

983. While previous MOVEit products required Progress's software to be installed and run on the customers' servers, MOVEit Cloud operates on Progress's servers, thus removing the need for customers to maintain their own servers.[59]

984. Accordingly, customers that use MOVEit Cloud do not need to update and patch software installed on their own servers because MOVEit Cloud is maintained by Progress and runs only on Progress servers.[60]

3. How MOVEit is used.

985. MOVEit software is used by different entities in order to transfer sensitive information.

986. Progress boasts that MOVEit is the "leading secure Managed File Transfer (MFT) software used by thousands of organizations around the world to provide complete visibility and control over file transfer activities. Whether deployed as-a-Service, in the Cloud, or on premises,

---

[56] *Id.*

[57] Brandon Butler, *File transfer systems adapting to today's cloudy conditions*, NetworkWorld (Nov. 13, 2012), https://www.networkworld.com/article/666073/cloud-computing-file-transfer-systems-adapting-to-today-s-cloudy-conditions.html.

[58] *MOVEit Cloud: Managed File Transfer-as-a-Service*, Progress: MOVEit, https://www.ipswitch.com/moveit-cloud (last visited Nov. 26, 2024).

[59] *Id.*

[60] *Id.*

MOVEit enables your organization to meet compliance standards, easily ensure the reliability of core business processes, and secure the transfer of sensitive data between partners, customers, users and systems."[61]

987. MOVEit helps information technology teams "at almost every federal civilian agency and military branch to securely transfer mission-critical information and assure the performance of their networked infrastructures and applications."[62]

988. Many businesses rely on third parties to provide useful software and code as elements of the supply chain for their own services or applications.

989. In this case, entities could either contract directly with Progress to use MOVEit software (either on-premises via MOVEit Transfer or online via MOVEit Cloud), or contract with a third-party which used MOVEit software. A variety of parties—such as direct users or vendors—thus used MOVEit software to effectuate file transfers. *See* Exhibit A (Updated Defendant Track Appendix A).

B. Progress warrants the security of its software.

990. Progress knows and intends that its customers use MOVEit software to transfer highly sensitive personally identifiable and protected health information ("Private Information").

991. Progress markets, advertises, and warrants MOVEit software as having industry-leading robust data security that complies with applicable data security laws and will keep Private Information from being compromised.

992. Regarding Progress's data security policies and practices, Progress states:

[61] *Managed File Transfer Software*, Progress: MOVEit, https://www.ipswitch.com/moveit (last visited Nov. 26, 2024).

[62] *FIPS Validated File Transfer Products*, Progress: MOVEit, https://www.ipswitch.com/industries/government-us-federal-government (last visited Nov. 26, 2024).

Progress MOVEit helps your organization meet cybersecurity compliance standards such as PCI-DSS, HIPAA, GDPR, SOC2 and more. Provide a more secure environment for your most sensitive files, while supporting the reliability of core business processes.[63]

* * *

The security of our customers' environments is paramount. Progress has a comprehensive cybersecurity program in place which includes a zero-trust cybersecurity architecture approach, compliance audits and verifications, source-code scanning, external penetration tests, third-party deep-dive code assessments as well as ongoing coordination with some of the industry's top cybersecurity researchers.

When vulnerabilities are found, we work quickly to mitigate the risk, issue appropriate patches and communicate directly with our customers, so they can take immediate action to harden their environments against those vulnerabilities.[64]

* * *

Employee Security Awareness

All employees undergo a regimen of security training throughout the year. Content is selected by committee and features such topics as General Security awareness, email security, phishing awareness, HIPAA ePHI Training, GDPR training, and secure coding.

Security Architecture Planning

Company Security Architecture planning is an ongoing activity managed by Corporate Information Security and Product Information Security Staff. Throughout the course of a given year risks are identified and tracked, existing information Security solutions are monitored, and new Security Technologies are researched for possible implementation. Standard approaches to perimeter Network Security, cloud infrastructure security, web and application security, authentication, and database security are just some of the disciplines we focus on. Our engineers work together

[63] *Managed File Transfer Software*, Progress: MOVEit, https://www.ipswitch.com/moveit (last visited Nov. 26, 2024).

[64] *Progress Trust Center*, Progress: MOVEit , https://www.progress.com/security (last visited Nov. 26, 2024).

within products and across products to ensure best practices in security design are implemented and maintained.

Security Defense

From corporate networks, to web applications, to cloud offerings, to employee computing environments, Progress employs a defense in depth strategy in the protection of our corporate assets and our customer environments. Network perimeter security, intrusion detection and prevention, anti-malware, anti-virus, server hardening, secure load balancing, secure authentication, encryption of data in transit, encryption of data at rest, stringent user access control, database security, security monitoring, and event management are just a few of the technologies involved in protecting our business and our customers.

* * *

Product Security

All software products at progress are developed a via the use of modern methodologies, techniques, technologies, and processes. Our software development life cycles employ Agile methodologies while including numerous waves of security planning and testing. These include security requirements planning, security design planning, code level security scanning, vulnerability scanning, and penetration testing.

Threat and Vulnerability Management

Ongoing threat and vulnerability management activities performed on all corporate assets and customer facing product environments. These activities include monitoring of key government and media outlets to stay apprised of emerging security issues, vulnerability scanning of internal and external systems, penetration testing of products and corporate environments.

Remediation Management

Progress subjects itself to a regular regimen of assessment activities to identify information security risks. Such activities may include self-initiated security assessments via a contracted 3rd party security firms, systems controls reviews by external industry authorities, or internal assessment activities using the expertise of existing staff. As such activities are conducted, any finding will be processed in a consistent manner that mitigates risk.

> **Security Incident Management**
>
> The Executive Security Committee at Progress has directed that an Incident Management function be operated that handles all corporate and customer related incident matters. In the case of an information security incident that threatens the availability, confidentiality, and integrity of information assets, information systems, and the networks that deliver the information, a response is conducted in a consistent manner. Appropriate leadership and technical resources are involved in any incident situation, in order to make key decisions and promptly restore any operations impacted. Exercises are performed on a recurring basis to ensure staff familiarity with procedures and identify any new lessons that should be incorporate into response plans.[65]

993. Regarding MOVEit Transfer's data security, Progress specifically states:

> **More Secure Managed File Transfer Software for the Enterprise**
>
> Leverage MOVEit Transfer's file encryption, security capabilities, tamper-evident logging, activity tracking and centralized access controls to help meet your operational requirements. Facilitate compliance with SLAs, internal governance requirements and regulations like PCI, HIPAA, CCPA/CPRA and GDPR.
>
> * * *
>
> **Transfer Sensitive Information More Securely**
>
> Help secure enterprise data in transit and at rest with advanced security features and encryption (FIPS 140-2 validated AES-256 cryptography). Better enforce user, system and file security policies while controlling the movement of sensitive files. Leverage user authentication, delivery confirmation, non-repudiation and hardened platform configurations.[66]
>
> * * *
>
> **Aid Secure End User Collaboration**
>
> When sensitive data is likely to be externally shared by end users, MOVEit's Ad Hoc, Secure Folder Sharing and MOVEit Client

[65] *Information Security Program Whitepaper*, Progress: Legal Info., https://www.progress.com/security/information-security-program-whitepaper (last visited Nov. 26, 2024).

[66] *More Secure Managed File Transfer Software for the Enterprise*, Progress: MOVEit, https://www.progress.com/moveit/moveit-transfer (last visited Nov. 26, 2024).

> provide a more secure, convenient and easy-to-use alternative to unsafe email and content collaboration. This allows IT teams to strengthen data security, visibility and audit trails and compliance with data protection regulations such as PCI, HIPAA, CCPA/CPRA and GDPR.
>
> * * *
>
> **Easily implement added security controls and establish an audit trail.**
>
> Because transfers are logged in a tamper-evident database, MOVEit Transfer helps facilitate compliance with SOC2, PCI-DSS, HIPAA, GDPR and other data privacy regulations. It provides pre-defined and customizable reports and logging of all data interactions, including files, events, people, policies and processes.
>
> * * *
>
> **Provide alternatives to risky transfer methods.**
>
> Improve the secure and compliant transfer of protected data by providing users with easy-to-use alternatives to risky transfer methods. Secure Folder Sharing provides a convenient, easy-to-use alternative to consumer-grade file sharing services. MOVEit Client helps provide access to secure transfers from Windows and MacOS desktops. MOVEit Ad-Hoc helps make secure file transfer easily accessible via email, either from Microsoft Outlook or a web browser. MOVEit Mobile enables access from iOS or Android devices.[67]

994. Progress "***guarantees*** the security of sensitive files both at-rest and in-transit."[68]

995. Progress, by marketing and advertising the MOVEit software as a solution for secure transfer and storage of files containing highly sensitive Private Information, knew or should have known that it was responsible for: keeping customers' files private; complying with industry standards related to data security and maintenance of its customers' files and the Private

[67] *Id.*

[68] *Applications & Experiences That Set You Apart*, Progress, https://d117h1jjiq768j.cloudfront.net/docs/default-source/default-document-library/progress-corporate-brochure-2023-rgb.pdf (last visited Nov. 26, 2024).

Information contained therein; ensuring the security of customers' files and the Private Information contained therein to protect them from unauthorized disclosure and exfiltration; and providing adequate notice to customers and individuals if their Private Information was disclosed without authorization.

C. The vulnerabilities in Progress's software.

1. SQL injection vulnerability.

996. MOVEit Transfer logs transfers in a SQL database that is also maintained by the customer on their network.[69]

997. SQL, developed in the 1970s and standing for "Structured Query Language," is one of the most popular programming languages for interacting with relational databases, databases that store data in tables made up of rows and columns. Many of the most popular relational database providers and implementations use SQL, including MySQL and Oracle. SQL commands use common English words such as INSERT, UPDATE, DELETE, etc., which make the language intuitive and easy to learn. An SQL engine takes an SQL query or statement as input, parses it into executable code, and then executes that code to return any matching rows in the database. As long as the SQL statement inputted can be parsed as valid SQL, the database can execute it.[70] Because SQL is used only to access a database, it is used alongside other server-side programming languages that perform other functions of a server, such as validating user input or creating web

[69] *MOVEit Transfer High Availability (HA) Data Sheet*, Progress: Resources, https://www.ipswitch.com/resources/data-sheets/moveit-transfer-high-availability (last visited Nov. 26, 2024).

[70] *What is SQL (Structured Query Language)?*, Amazon Web Servs., https://aws.amazon.com/what-is/sql/ (last visited Nov. 26, 2024).

pages. Other server-side programming languages also have built-in functions that can create SQL queries and send queries to an SQL engine.[71]

998. When a customer logs into or uses the MOVEit Transfer web application, they may input some information into form fields (*e.g.*, email, password, or other user-inputted information), which is then transmitted to the MOVEit Transfer server running on the customer's network to be interpreted and processed by the MOVEit Transfer software. Some user input is passed to the MOVEit Transfer SQL database as part of the query (*e.g.*, comparing credentials inputted by a user to credentials stored in the database, or searching a table for a certain record).[72]

999. The simplicity of SQL makes it both very useful and highly vulnerable to exploitation through SQL injection.[73]

1000. SQL injection is described in the Common Weakness Enumeration database as follows:

> Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, possibly including execution of system commands.
>
> SQL injection has become a common issue with database-driven web sites. The flaw is easily detected, and easily exploited, and as such, any site or product package with even a minimal user base is likely to be subject to an attempted attack of this kind. This flaw

[71] *See, e.g.*, *Create a SQL Server Database programmatically by using ADO.NET and Visual C# .NET*, Microsoft (May 7, 2022), https://learn.microsoft.com/en-us/troubleshoot/developer/visualstudio/csharp/language-compilers/create-sql-server-database-programmatically.

[72] Kinza Yasar et al., *Definition: SQL injection (SQLi)*, TechTarget (Apr. 2023), https://www.techtarget.com/searchsoftwarequality/definition/SQL-injection.

[73] *Id.*

> depends on the fact that SQL makes no real distinction between the control and data planes.[74]

1001. SQL injection works by submitting plain-text malicious SQL code as input into a web application so that a web application's server will unwittingly execute the malicious code when it processes the input.[75]

1002. The malicious code may be used to reveal or alter data in the database that should not be allowed based on the limited input that the web application is expecting.[76]

1003. SQL injection takes advantage of the simplicity of SQL engines, which will interpret and execute any valid SQL that is passed to them.[77]

1004. For example, an SQL database may store information about customers associated with a "CustomerID" field. A form may prompt a user to enter a CustomerID so that the server can retrieve information about a customer from the database. The server would expect a user input for a "CustomerID" such as "1000." The server will then take the user input and insert it into a plain-text SQL query that compares the table column "CustomerID" to the input of "1000" and return any table rows for which the statement "CustomerID=1000" is true. The query may look like this: "SELECT name, address, account_number FROM customers WHERE CustomerID=1000." This query would then be parsed and executed by the SQL engine to "select" the data fields "name, address, account_number" for any records "where" the "CustomerID" is equal to 1000. But the structure of this query is vulnerable to SQL injection because any user input

---

[74] *CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')*, Common Weakness Enumeration: CWE-Individual Dictionary Definition 4.14 (Feb. 29, 2024), https://cwe.mitre.org/data/definitions/89.html.

[75] Kinza Yasar et al., *Definition: SQL injection (SQLi)*, TechTarget (Apr. 2023), https://www.techtarget.com/searchsoftwarequality/definition/SQL-injection.

[76] *Id.*

[77] *Id.*

is inserted directly into the plain text SQL query (*e.g.*, the user input "1000"). So, if instead of just "1000," the user input is "1000 OR 1=1," then the new query would look like this: "SELECT name, address, account_number FROM customers WHERE CustomerID=1000 OR 1=1." Rather than retrieving records where the CustomerID is 1000, this query will return any rows in which the statement "CustomerID=1000 OR 1=1" is true. Because "1=1" is always true, this statement is true for all rows in the table, regardless of whether the CustomerID for the row is equal to 1000, and therefore all rows will be returned. Depending on the design of the server, instead of being shown data from the row associated with the CustomerID of 1000, the user would be shown the first row of the table, or potentially all rows of the table, which the user may not be authorized to view. This is a rudimentary example of how SQL injection can cause a server to provide or alter more data than intended or than the user is authorized to access.[78]

1005. SQL injection may also involve other SQL commands that can completely change the nature of the original query so the user can access or alter any information throughout the database.[79]

> Consider the following code that concatenates user input with SQL syntax:
>
> ```
> $name = $_REQUEST['name'];
>
> $email = $_REQUEST['email'];
>
> $sql = "INSERT INTO CustomerTable (Name,
> Email) VALUES ('$name', '$email')";
> ```

[78] *Id.*

[79] *How and Why to Use Parameterized Queries*, Microsoft (Mar. 23, 2019), https://techcommunity.microsoft.com/t5/sql-server-blog/how-and-why-to-use-parameterized-queries/ba-p/383483.

Now suppose a user enters the following data:

The resulting SQL query (defined by $sql) is the following:

```
INSERT INTO CustomerTable (Name, Email)
VALUES ('Brian', 'bswan@microsoft.com');
DROP TABLE CustomerTable; PRINT
'Gotcha!'--')
```

1006. In the above example, the user input fields "name" and "email" are inserted directly into an SQL query that will then insert those values into the table "CustomerTable." However, in the "email" form input, the user puts a semi-colon—the symbol for the end of an SQL query—and then continued with a completely new SQL query: "DROP TABLE CustomerTable." A "DROP" command will delete the referenced table. When this user input is concatenated with the SQL statement and executed by the SQL engine, the table "CustomerTable" will be deleted from the database. Other commands could be used in a similar manner to alter the database, such as INSERT or UPDATE.[80]

1007. SQL injection only works when a server receiving user input "trusts" that user input and enters it directly into a plain text SQL statement to be parsed and executed by the database.[81]

[80] *Id.*

[81] Kinza Yasar, et al., *Definition: SQL injection (SQLi)*, TechTarget (Apr. 2023), https://www.techtarget.com/searchsoftwarequality/definition/SQL-injection.

1008. It is bad practice to trust any user input, even from authorized and trusted users, because any input can contain unexpected characters or SQL code that would then be passed directly to the database.[82]

1009. Rather, user input should be validated and "sanitized" to ensure it does not contain any prohibited characters or SQL commands and matches the format expected by the server.[83]

1010. In the above example, if the server were programmed to validate user input when querying the CustomerID field to ensure that any input is just a four-digit number, then when the server receives the input "1000 OR 1=1," the server would see that this string is not a four-digit number, reject it, and not insert the plain text input into the SQL query, thus preventing the SQL injection.[84]

1011. Another common method for sanitizing user input is to "escape" special characters so they are interpreted by the SQL parser as plain text instead of SQL code.[85]

1012. An escape function, when applied to a user input string, will replace special characters with neutral characters that the SQL parser will not interpret as SQL code. For example, an escape function may cause special characters to be preceded by a backslash ("\"), which signals

[82] *Id.*; *see also Deserialization risks in use of BinaryFormatter and related types*, Microsoft Build: Learn .NET (Apr. 4, 2023), https://learn.microsoft.com/en-us/dotnet/standard/serialization/binaryformatter-security-guide.

[83] *AO3:2021 - Injection*, Open Worldwide Application Sec. Project: OWASP Top 10 (2021), https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html#defense-option-4-strongly-discouraged-escaping-all-user-supplied-input.

[84] Kinza Yasar et al., *Definition: SQL injection (SQLi)*, TechTarget (Apr. 2023), https://www.techtarget.com/searchsoftwarequality/definition/SQL-injection.

[85] *Defense Option 4: STRONGLY DISCOURAGED: Escaping All User-Supplied Input*, OWASP Cheat Sheet Series: SQL Injection Prevention Cheat Sheet, https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html#defense-option-4-strongly-discouraged-escaping-all-user-supplied-input (last visited Nov. 26, 2024).

to the SQL parser that the succeeding character should be interpreted as a plain text string, not as SQL code.[86]

1013. Because escaping is a fairly rudimentary way to sanitize user input and only applies to certain characters, it cannot guarantee that SQL injection can be prevented in all cases.[87]

1014. The antiquated manner of constructing SQL statements—concatenating SQL code with plain text user input—is vulnerable to SQL injection because user input might contain SQL code, so any malicious code in the user input is treated as valid SQL.[88]

1015. Modern and secure SQL databases, and the programming languages that interact with them, have basic tools built in called "parameterized" or "prepared" statements that can make SQL injection impossible when used properly.[89]

1016. Use of parameterized statements separates SQL statements from plain text user input by performing different functions with each. The SQL engine first compiles a pre-written SQL query with defined placeholders for user input. The SQL engine then inserts the plain text user input into those placeholders. The interpretation of SQL and user input in separate steps ensures that SQL is interpreted as SQL and user input is interpreted as plain text. Therefore, even

---

[86] *STRING_ESCAPE (Transact-SQL)*, Microsoft Build: Learn .NET (Jun. 1, 2023), https://learn.microsoft.com/en-us/sql/t-sql/functions/string-escape-transact-sql.

[87] *Defense Option 4: STRONGLY DISCOURAGED: Escaping All User-Supplied Input*, OWASP Cheat Sheet Series: SQL Injection Prevention Cheat Sheet, https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html#defense-option-4-strongly-discouraged-escaping-all-user-supplied-input (last visited Nov. 26, 2024).

[88] *How to prevent SQL Injection Vulnerabilities: How Prepared Statements Work*, Sec. Journey: Blog (Feb. 11, 2020), https://www.securityjourney.com/post/how-to-prevent-sql-injection-vulnerabilities-how-prepared-statements-work.

[89] *Query Parameterization Cheat Sheet*, OWASP Cheat Sheet Series: SQL Injection Prevention Cheat Sheet, https://cheatsheetseries.owasp.org/cheatsheets/Query_Parameterization_Cheat_Sheet.html (last visited Nov. 26, 2024).

if malicious code is inputted, it cannot be interpreted and executed as SQL code, but rather, is always treated as plain text.[90]

1017. The following example using the PHP programming language illustrates how parameterized statements easily separate code from input to prevent SQL injection[91]:

```
$stmt = $mysqli->prepare("SELECT * FROM
users WHERE user = ? AND password = ?");

$stmt->bind_param("ss", $username,
$password);

$stmt->execute();
```

1018. In the above example, SQL is used to select a row from the table "users" where the "user" and "password" match the user input values stored in the variables "$username" and "$password." First, the "prepare" function is used to prepare the SQL query with placeholders (question marks). Only the text within the "prepare" function is interpreted as SQL. Then the "bind_param" function is used to insert the user input—stored in the variables "$username" and "$password"—into the prepared query's predefined placeholders. User input that is binded to the prepared query is interpreted as plain text. Thus, even if malicious code were inputted into the "username" or "password" fields, the server would treat the malicious code as plain text, not as executable SQL code.[92]

---

[90] *SQL Injection Prevention Cheat Sheet*, OWASP Cheat Sheet Series, https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html (last visited Nov. 26, 2024).

[91] *How to prevent SQL Injection Vulnerabilities: How Prepared Statements Work,* Sec. Journey: Blog (Feb. 11, 2020), https://www.securityjourney.com/post/how-to-prevent-sql-injection-vulnerabilities-how-prepared-statements-work.

[92] *Id.*

1019. Parameterized statements are fundamental tools for developers who code with SQL.[93]

1020. Sanitizing user input and using parameterized statements are easy and common ways to ensure that SQL injection is impossible.[94]

1021. Sanitizing user input and using parameterized statements are industry standards and generally recognized best practices when working with user input and SQL databases.[95]

1022. SQL injection is the third most critical security risk to web applications according to the Open Worldwide Application Security Project ("OWASP"), a nonprofit foundation that sets industry standards for software security.[96]

1023. SQL injection has been documented, understood, and easy to prevent since 1998.[97]

1024. Structuring code to avoid SQL injection is recognized as an industry standard because it is well understood, easy to accomplish, and averts risks of data theft:

a. The popular website howtogeek.com states: "A SQL injection attack is caused by negligent and irresponsible application coding and is completely

[93] *SQL Injection Prevention Cheat Sheet*, OWASP Cheat Sheet Series, https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html (last visited Nov. 26, 2024).

[94] Kinza Yasar et al., *Definition: SQL injection (SQLi)*, TechTarget (Apr. 2023), https://www.techtarget.com/searchsoftwarequality/definition/SQL-injection.

[95] *AO3:2021 – Injection*, *supra* note 51; *How to use the OWASP Top 10 as a standard*, Open Worldwide Application Sec. Project: OWASP Top 10 (2021), https://owasp.org/Top10/A00_2021_How_to_use_the_OWASP_Top_10_as_a_standard/.

[96] *OWASP Top 10*, Open Worldwide Application Sec. Project, https://owasp.org/www-project-top-ten/; https://owasp.org/about/ (last visited Nov. 5, 2024).

[97] Kinza Yasar et al., *Definition: SQL injection (SQLi)*, TechTarget (Apr. 2023), https://www.techtarget.com/searchsoftwarequality/definition/SQL-injection.

preventable (which we will cover in a moment), however the extent of the damage which can be done depends on the database setup."[98]

b. The online journal CSO Online states: "The good news? SQL injection is the lowest of the low-hanging fruit for both attackers and defenders. It isn't some cutting edge NSA Shadow Brokers kit, it's so simple a three-year old can do it. This is script kiddie stuff—and fixing your web application to mitigate the risk of SQL injection is so easy that failure to do so looks more and more like gross negligence."[99]

c. BankInfoSecurity.com states: "'SQL attacks persist because they are simple by nature,' Group-IB's Rostovcev said. 'Companies often overlook how critical input security and data validation are, which leads to vulnerable coding practices, outdated software and improper database settings. The negligence creates the perfect landscape for SQL injection attacks on public-facing web applications.'"[100]

2. .NET BinaryFormatter.Deserialize vulnerability.

1025. The MOVEit Transfer software performs file uploads with code written in the .NET Framework.[101]

1026. .NET is a free and open-source software framework developed and maintained by Microsoft.[102]

[98] Jason Faulkner, *How Hackers Take Over Web Sites with SQL Injection and DDoS*, How To Geek (Sept. 28, 2016), https://www.howtogeek.com/97971/htg-explains-how-hackers-take-over-web-sites-with-sql-injection-ddos/

[99] J.M. Porup, *What is SQL injection? How these attacks work and how to prevent them*, CSO (Oct. 2, 2018), .https://www.csoonline.com/article/564663/what-is-sql-injection-how-these-attacks-work-and-how-to-prevent-them.html.

[100] Matthew J. Schwartz, *Hackers Keep Winning by Gambling on SQL Injection Exploits*, Bank Info Security (Dec. 14, 2023), https://www.bankinfosecurity.com/hackers-keep-winning-by-gambling-on-sql-injection-exploits-a-23882.

[101] Zach Hanley, *MOVEit Transfer CVE-2023-34362 Deep Dive and Indicators of Compromise*, Horizon3.ai: Attack Blogs (June 9, 2023), https://www.horizon3.ai/attack-research/attack-blogs/moveit-transfer-cve-2023-34362-deep-dive-and-indicators-of-compromise/.

[102] *Download.NET*, Microsoft: .NET, https://dotnet.microsoft.com/en-us/download (last visited Nov. 26, 2024).

1027. Within MOVEit Transfer's file upload code, a .NET BinaryFormatter type and a Deserialize function are used when storing and recalling files while they are in the process of being uploaded.[103]

1028. BinaryFormatter is used to "[s]erialize[] and deserialize[] an object, or an entire graph of connected objects, in binary format."[104]

1029. BinaryFormatter is used to save (serialize) and recall (deserialize) binary objects as exact copies and, by design, does not validate that the object is valid.[105]

1030. Deserialization of untrusted user input therefore introduces risks that an object is not a well-formed or validated object, potentially containing malicious code.[106]

1031. Use of the BinaryFormatter type "is a classic .NET deserialization vulnerability."[107]

1032. "BinaryFormatter was implemented before deserialization vulnerabilities were a well-understood threat category. As a result, the code does not follow modern best practices."[108]

---

[103] Zach Hanley, *MOVEit Transfer CVE-2023-34362 Deep Dive and Indicators of Compromise*, Horizon3.ai: Attack Blogs (June 9, 2023), https://www.horizon3.ai/attack-research/attack-blogs/moveit-transfer-cve-2023-34362-deep-dive-and-indicators-of-compromise/.

[104] *BinaryFormatter Class*, Microsoft Build: Learn .NET, https://learn.microsoft.com/en-us/dotnet/api/system.runtime.serialization.formatters.binary.binaryformatter (last visited Nov. 26, 2024).

[105] *Sterilization in .NET*, Microsoft Build: Learn .NET (Oct. 25, 2023), https://learn.microsoft.com/en-us/dotnet/standard/serialization/.

[106] *Deserialization of untrusted data*, Open Worldwide Application Sec. Project, https://owasp.org/www-community/vulnerabilities/Deserialization_of_untrusted_data (last visited Nov. 26, 2024).

[107] Zach Hanley, *MOVEit Transfer CVE-2023-34362 Deep Dive and Indicators of Compromise*, Horizon3.ai: Attack Blogs (June 9, 2023), https://www.horizon3.ai/attack-research/attack-blogs/moveit-transfer-cve-2023-34362-deep-dive-and-indicators-of-compromise/.

[108] *Deserialization risks in use of BinaryFormatter and related types*, Microsoft Build: Learn .NET (Apr. 4, 2023), https://learn.microsoft.com/en-us/dotnet/standard/serialization/binaryformatter-security-guide.

1033. Microsoft advises regarding use of BinaryFormatter and Deserialize[109]:

> The BinaryFormatter type is dangerous and is ***not*** recommended for data processing. Applications should stop using BinaryFormatter as soon as possible, even if they believe the data they're processing to be trustworthy. BinaryFormatter is insecure and can't be made secure.
>
> . . .
>
> Deserialization vulnerabilities are a threat category where request payloads are processed insecurely. An attacker who successfully leverages these vulnerabilities against an app can cause denial of service (DoS), information disclosure, or remote code execution inside the target app. This risk category consistently makes the OWASP Top 10.
>
> . . .
>
> As a simpler analogy, assume that calling BinaryFormatter.Deserialize over a payload is the equivalent of interpreting that payload as a standalone executable and launching it.
>
> . . .
>
> The BinaryFormatter.Deserialize method is **never** safe when used with untrusted input. We strongly recommend that consumers instead consider using one of the alternatives outlined later in this article.
>
> . . .
>
> We recommend that BinaryFormatter consumers perform individual risk assessments on their apps. It is the consumer's sole responsibility to determine whether to utilize BinaryFormatter. If you're considering using it, you should risk-assess the security, technical, reputation, legal, and regulatory consequences.

1034. "[C]alling BinaryFormatter.Deserialize over a payload is the equivalent of interpreting that payload as a standalone executable and launching it."[110]

[109] *Id.*

[110] *Id.*

1035. An unauthorized user could therefore upload a malicious program to a server that uses the BinaryFormatter.Deserialize function, and the server would unwittingly execute the code with administrator permissions, known as remote code execution.[111]

1036. Due to these critical security vulnerabilities, recent versions of .NET now flag any use of BinaryFormatter.Deserialize as an error.[112]

1037. The API documentation page for BinaryFormatter immediately warns developers of the vulnerability: "BinaryFormatter serialization is obsolete and should not be used."[113]

1038. Ultimately, Microsoft recommends: "Stop using BinaryFormatter in your code."[114]

1039. OWASP ranked "Insecure Deserialization" as number 8 on their 2017 Top 10 list of software security vulnerabilities based on an industry survey.[115]

1040. OWASP now ranks "Vulnerable and Outdated Components" as the sixth ranking web application security risk.[116]

---

[111] Zach Hanley, *MOVEit Transfer CVE-2023-34362 Deep Dive and Indicators of Compromise*, Horizon3.ai: Attack Blogs (June 9, 2023), https://www.horizon3.ai/attack-research/attack-blogs/moveit-transfer-cve-2023-34362-deep-dive-and-indicators-of-compromise/.

[112] *BinaryFormatter serialization methods are obsolete and prohibited in ASP.NET apps*, Microsoft Build: Learn .NET (May 17, 2023), https://learn.microsoft.com/en-us/dotnet/core/compatibility/serialization/5.0/binaryformatter-serialization-obsolete.

[113] *BinaryFormatter Class*, Microsoft Build: Learn .NET, https://learn.microsoft.com/en-us/dotnet/api/system.runtime.serialization.formatters.binary.binaryformatter (last visited Nov. 26, 2024).

[114] *BinaryFormatter serialization methods are obsolete and prohibited in ASP.NET apps*, Microsoft Build: Learn .NET (May 17, 2023), https://learn.microsoft.com/en-us/dotnet/core/compatibility/serialization/5.0/binaryformatter-serialization-obsolete.

[115] *A8:2017-Insecure Deserialization*, Open Worldwide Application Sec. Project: OWASP Top 10 (2017), https://owasp.org/www-project-top-ten/2017/A8_2017-Insecure_Deserialization.html.

[116] *OWASP Top Ten*, Open Worldwide Application Sec. Project, https://owasp.org/www-project-top-ten/ (last visited Nov. 26, 2024).

1041. The BinaryFormatter.Deserialize vulnerability has been documented, understood, and easy to prevent since at least 2017, when the tool YSoSerial.Net was developed. YsoSerial.Net is "[a] proof-of-concept tool for generating payloads that exploit unsafe .NET object deserialization." YSoSerial.Net has 27 contributors to its open-source codebase, has been continuously maintained, and has approximately 3,000 stars on GitHub.[117]

1042. Microsoft recommends use of YSoSerial.Net "for research into how adversaries attack apps that utilize BinaryFormatter."[118]

3. Insecure key storage vulnerability.

1043. MOVEit Transfer encrypts files both in transit and at rest so they cannot be viewed at any time without the appropriate encryption key.[119]

1044. Encrypting data at rest is a common data security practice[120] specifically recommended to mitigate SQL injection attacks.[121] Encrypting files and databases at rest prevents

[117] pwntester (Alvaro Muñoz), *ysoserial.net*, GitHub (Oct. 17, 2023), https://github.com/pwntester/ysoserial.net.

[118] *Deserialization risks in use of BinaryFormatter and related types*, Microsoft Build: Learn .NET (Apr. 4, 2023), https://learn.microsoft.com/en-us/dotnet/standard/serialization/binaryformatter-security-guide.

[119] *Introduction, MOVEit Transfer 2023.1 Adm'r Guide*, Progress: Prod. Documentation (Apr. 21, 2022), https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2023/page/Introduction.html.

[120] *See, e.g.*, Scott Myers, *Securing Data at Rest with Encryption*, Ingalls (Apr. 20, 2022), https://blog.iinfosec.com/securing-data-at-rest-with-encryption; *SQL Injection Attacks (SQLi)*, Rapid 7, https://www.rapid7.com/fundamentals/sql-injection-attacks/ (last visited Nov. 6, 2024); Sonakshi, et al., *Prevention of SQL Injection Attacks using RC4 and Blowfish Encryption Techniques*, 5 Int'l J. of Engineering Research & Tech., 25, 25-29 (2016), https://www.ijert.org/research/prevention-of-sql-injection-attacks-using-rc4-and-blowfish-encryption-techniques-IJERTV5IS060092.pdf.

[121] Sonakshi, et al., *Prevention of SQL Injection Attacks using RC4 and Blowfish Encryption Techniques*, 5 Int'l J. of Engineering Research & Tech. 6 (June 2016), https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1105&context=msia_etds.

threat actors who gain access to a system from accessing sensitive data on the system without a cryptographic key and is required or recommended by numerous standards, including PCI-Data Security Standards,[122] SOC 2,[123] and NIST SP 800-53.[124] The standard NIST SP 800-53 explicitly recommends encrypting data at rest in section SC-28.[125]

1045. PCI-DSS specifically recommends encryption of data and data masking. Protection methods such as encryption, truncation, masking, and hashing are critical components of account data protection. If an intruder circumvents other security controls and gains access to encrypted account data, the data is unreadable without the proper cryptographic keys and is unusable to that intruder.

1046. However, MOVEit Transfer does not store and retrieve encryption keys in a secure manner.

1047. "MOVEit Transfer manages the encryption keys transparently. Each file is encrypted using a file-specific encryption key derived in-part from the Org passphrase specified during deployment."[126]

1048. "Transparent Encryption refers to a method of encrypting data at rest, where the encryption and decryption process is transparent to the user and the application. This means that

---

[122] *Document Library*, PCI, https://east.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss (last visited Nov. 6, 2024).

[123] *SOC2 Compliance – The Definitive Guide*, A-LIGN, https://www.a-lign.com/resources/soc-2-the-definitive-guide (last visited Nov. 6, 2024).

[124] NIST, *NIST SP 800-53 – Security and Privacy Controls for Information Systems and Organizations*, U.S. Dep't of Commerce (Sept. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[125] *Id.*

[126] *What system encryption does MOVEit Transfer (MIT) use*, Progress (Feb. 2, 2024), https://community.progress.com/s/article/what-system-encryption-does-moveit-transfer-mit-use.

the user or application does not need to take any explicit action to encrypt or decrypt the data. The process is handled automatically by the underlying storage or database management system."[127]

1049. Encryption keys are stored on the MOVEit Transfer server. "Certain fields in [MOVEit Transfer's] MySQL database are encrypted, but the MySQL database as-a-whole is not."[128]

1050. "Where possible, encryption keys should themselves be stored in an encrypted form" using both data encryption keys and key encryption keys which are stored separately.[129]

1051. MOVEit does not separately encrypt data encryption keys with key encryption keys. This is evident based on the ability of an authenticated user to decrypt data without providing a password or separate key encryption key.[130]

1052. Secure storage of encryption keys is an industry standard which should be accomplished by separation of keys and data and encrypting stored keys.[131]

1053. "Where possible, encryption keys should be stored in a separate location from encrypted data. For example, if the data is stored in a database, the keys should be stored in the filesystem. This means that if an attacker only has access to one of these (for example through

---

[127] *What is Transparent Encryption?*, Fortanix, https://www.fortanix.com/faq/encryption/what-is-transparent-encryption (last visited Dec. 4, 2024).

[128] *What system encryption does MOVEit Transfer (MIT) use*, Progress (Feb. 2, 2024), https://community.progress.com/s/article/what-system-encryption-does-moveit-transfer-mit-use.

[129] Cryptographic Storage Cheat Sheet, OWASP, https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html (last visited Dec. 4, 2024).

[130] Tr33, Understanding CVE-2023-34362: A critical MOVEit Transfer vulnerability, Hack The Box (Oct. 16, 2023), https://www.hackthebox.com/blog/cve-2023-34362-explained.

[131] Cryptographic Storage Cheat Sheet, OWASP, https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html (last visited Dec. 4, 2024); *Recommendation for Key Management*, NIST (May 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf.

directory traversal or SQL injection), they cannot access both the keys and the data. Depending on the architecture of the environment, it may be possible to store the keys and data on separate systems, which would provide a greater degree of isolation."[132]

1054. "Where possible, encryption keys should themselves be stored in an encrypted form" using Data Encryption Keys to encrypt the data and Key Encryption Keys to encrypt the Data Encryption Keys. "For this to be effective, the KEK must be stored separately from the DEK. The encrypted DEK can be stored with the data, but will only be usable if an attacker is able to also obtain the KEK, which is stored on another system."[133]

1055. Further, there are various means to keep encryption keys protected, including[134]:

- A physical Hardware Security Module (HSM).
- A virtual HSM.
- Key vaults such as Amazon KMS or Azure Key Vault.
- An external secrets management service such as Conjur or HashiCorp Vault.
- Secure storage APIs provided by the ProtectedData class in the .NET framework.

1056. "Poor key management practices render encryption useless, leaving data exposed."[135]

---

[132] *Id*.

[133] *Id.*

[134] *Id*.

[135] *Key Management Best Practices: A Practical Guide*, SSL.com (May 3, 2024), https://www.ssl.com/article/key-management-best-practices-a-practical-guide/.

D. CL0P exploited the MOVEit vulnerabilities to steal data from hundreds of organizations.

1. CL0P ransomware gang.

1057. CL0P, also known as TA505, is a Russian cybercriminal ransomware gang.[136]

1058. CL0P is part of the broader ransomware-as-a-service ("RaaS") ecosystem, where ransomware is developed and maintained by a central group, while affiliates carry out attacks in exchange for a share of the profits.[137] CL0P is primarily motivated by financial gain.[138]

1059. Emerging in February 2019, CL0P primarily used "double extortion" tactics whereby CL0P would hack into an organization's network, encrypt the data therein, and then exfiltrate and threaten to leak the data on the dark web. The only way for the organization to regain access to their data and prevent it from being leaked was to pay a ransom.[139]

1060. In 2021, CL0P began to rely primarily on stealing and ransoming data rather than encrypting data.[140]

---

[136] Sean Lyngaas, *Russian-speaking cyber gang claims credit for hack of BBC and British Airways employee data*, CNN (June 7, 2023, 12:56 PM), https://www.cnn.com/2023/06/07/tech/clop-russia-moveit-hack-payroll-uk/index.html; *#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, Cybersecurity & Infrastructure Sec. Agency (CISA) (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[137] *#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, Cybersecurity & Infrastructure Sec. Agency (CISA) (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[138] Office of Information Security, *HC3: Threat Actor Profile*, HHS (June 13, 2023), https://www.hhs.gov/sites/default/files/threat-profile-june-2023.pdf.

[139] *#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, Cybersecurity & Infrastructure Sec. Agency (CISA) (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[140] *Id.*

1061. CL0P operates the dark website >_CLOP^_-LEAKS, on which it posts ransom demands and leaks stolen data.[141]

1062. CL0P "conducted zero-day-exploit-driven campaigns against Accellion File Transfer Appliance (FTA) devices in 2020 and 2021, and Fortra/Linoma GoAnywhere MFT servers in early 2023."[142]

1063. "Beyond CL0P ransomware, TA505 is known for frequently changing malware and driving global trends in criminal malware distribution. Considered to be one of the largest phishing and malspam distributors worldwide, TA505 is estimated to have compromised more than 3,000 U.S.-based organizations and 8,000 global organizations."[143]

2. CL0P is a well-known danger, posing a threat to individuals who are impacted by its exploits for years to come.

1064. CL0P is considered particularly dangerous due to its adaptability, strategic targeting of high-impact systems, and the sophistication of its ransomware attacks.

1065. CL0P has shown a solid ability to discover and exploit zero-day vulnerabilities, particularly in widely used software. This skill gives them access to sensitive data and systems before most defenses know the threat.[144]

1066. CL0P strategically focuses on supply chains, targeting software used by many organizations, which maximizes their reach and impact. By compromising a single software

---

[141] Riam Kim-Mcleod, *Clop Leaks: First Wave of Victims Named*, ReliaQuest: Blog (July 28, 2023, 10:00 AM), https://www.reliaquest.com/blog/clop-leaks-first-victims/.

[142] *#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, Cybersecurity & Infrastructure Sec. Agency (CISA) (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[143] *Id.*

[144] *Dark Web Threat Profile: CLOP Ransomware*, SOCRadar, https://socradar.io/dark-web-threat-profile-clop-ransomware/ (last updated Aug. 7, 2023).

vendor, they gain access to potentially thousands of clients using the same software, creating widespread effects and significant disruption.[145]

1067. CL0P has consistently targeted industries with high-value data, such as healthcare, finance, and government, increasing the potential impact of its attacks. This targeting amplifies the risks for sensitive data exposure, regulatory penalties, and disruption of critical services.[146]

1068. CL0P collects sensitive data through ransomware attacks so that the data can be ransomed, sold, shared, or otherwise used maliciously on the dark web.[147]

1069. CL0P also uses stolen data to assemble detailed dossiers containing sensitive information about organizations and their stakeholders to increase leverage on victims. These dossiers can include:

a. Stolen internal data: Employee credentials, financial information, and internal documents.

b. Publicly available data: Social media profiles, company press releases, and personal information of key executives combined with stolen data to create a comprehensive profile.

1070. Once they possess sensitive data, CL0P can use it to extort victims through threats of public exposure or sale on dark web sites to other cybercriminals, who may use the data for further attacks, fraud, or identity theft.[148]

1071. CL0P uses double or triple extortion to obtain the most leverage on their victims. First, CL0P demands a ransom for decrypting important data, followed by a second ransom for not

[145] *Id.*

[146] *Id.*

[147] Janus Agcaoili et al., *Ransomware Double Extrotion and Beyond: Revil, Clop, and Conti*, Trend (June 15, 2021), https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti.

[148] *Id.*

leaking the data to the dark web. Sometimes, CL0P adds a third layer, directly contacting customers or stakeholders to increase pressure.[149]

1072. CL0P may sell the stolen information on dark web markets to other threat actors, making the data available for identity theft, fraud, and secondary attacks.[150]

1073. CL0P can post the data on their leak sites or popular dark web forums, ensuring reputational damage for the victim and decreasing their trustworthiness.[151]

3. Exploiting MOVEit Transfer vulnerabilities.

1074. MOVEit Transfer was defective and vulnerable to SQL injection because it did not sanitize user input, use parameterized statements, or follow other industry data security standards to prevent malicious code from being remotely inputted into its database.[152]

1075. Analysis of the "guestaccess.aspx" login page within the MOVEit Transfer code revealed an "SQL query [made] from a concatenated string of several arguments passed in"[153]:

```
SELECT Username, Permissions, LoginName, Email
FROM users WHERE InstID=9389 AND Deleted=0 AND
(Email='<EmailAddress>' OR Email LIKE
(%EscapeLikeForSQL(<EmailAddress>)) or Email
LIKE (EscapeLikeForSQL(<EmailAddress>));
```

[149] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a; https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransomwares-double-extortion-tactics-and-how-to-protect-enterprises-against-them; Janus Agcaoili et al., *Ransomware Double Extrotion and Beyond: Revil, Clop, and Conti*, Trend (June 15, 2021), https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti.

[150] Janus Agcaoili et al., *Ransomware Double Extrotion and Beyond: Revil, Clop, and Conti,* Trend (June 15, 2021), https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti.

[151] *Id.*

[152] Zach Hanley, *MOVEit Transfer CVE-2023-34362 Deep Dive and Indicators of Compromise*, Horizon3.ai: Attack Blogs (June 9, 2023), https://www.horizon3.ai/attack-research/attack-blogs/moveit-transfer-cve-2023-34362-deep-dive-and-indicators-of-compromise/.

[153] *Id.*

1076. There are three comparisons in the SQL query that compare a user-inputted value "<EmailAddress>" to a table column "Email."[154]

1077. Two of the comparisons escape the user input before comparing it to the table using the function "EscapeLikeForSQL."[155]

1078. But the other comparison does not escape the user input, instead simply comparing the user input "<EmailAddress>" to the table column "Email" one-to-one[156]:

```
Email='<EmailAddress>'
```

1079. An unauthorized user could access a MOVEit Transfer database by inputting malicious code into a form field that prompts a user to enter an email address, and the malicious code would be inputted into the above plain text SQL query where the unescaped "<EmailAddress>" user input is included.[157]

1080. The malicious code would be executed because the MOVEit Transfer software did not sanitize the user input nor did it prepare the SQL query as a parameterized statement to separate code execution from user input.[158]

1081. This vulnerability gives unauthorized users "the ability to read and write any data within the MOVEit database."[159]

---

[154] *Id.*

[155] *Id.*

[156] *Id.*

[157] *Id.*

[158] *Id.*

[159] *Id.*

1082. The unauthorized user can then pose as a logged-in user by sending a request to the "guestaccess.aspx" page of the MOVEit Transfer server with fake credentials embedded with malicious SQL code.[160]

1083. When the server attempts to authenticate the fake credentials by executing the above query, it will execute the malicious SQL code.[161] The defective design of MOVEit allows a hacker to exploit this vulnerability, which results in automatic execution of the malicious SQL code.

1084. The unauthorized user then leverages a "federated login flow," which is a system that allows users to log-in to the MOVEit Transfer server using credentials for a third-party account, such as a Microsoft Outlook account. The federated login flow works by sending a JSON web token to the "/api/v1/auth/token" API endpoint of the MOVEit Transfer server containing a signature and a link to a trusted certificate to verify the credentials from the third-party account.[162]

1085. The SQL injection can be used to configure the MOVEit Transfer server to accept a federated login certificate from an untrusted source.[163]

1086. The unauthorized user can then send a JSON web token to the server with a fake certificate and "obtain an access token for the sysadmin user."[164]

1087. Once the unauthorized user has administrator permissions, they can access MOVEit Transfer functions for uploading and downloading files.[165]

---

[160] *Id.*

[161] *Id.*

[162] *Id.*

[163] *Id.*

[164] *Id.*

[165] *Id.*

1088. The unauthorized user can then download files from the MOVEit Transfer server through the MOVEit Transfer client, web app, or API.[166]

1089. With root access to the server—not merely administrator permissions within the MOVEit Transfer software—the unauthorized user can compress and bulk download files saved on the server more easily and efficiently.[167]

1090. Gaining root access to the server involves taking advantage of a vulnerability in the file upload API endpoint at "/api/v1/folders/<folder_id>/files?uploadType=resumable&fileId=<file_id>."[168]

1091. "When initiating [a] file upload [through MOVEit Transfer], you can optionally provide a Comment. This comment is encrypted with that organization specific key."[169]

1092. The unauthorized user sends a request to the MOVEit Transfer file upload endpoint, which logs the upload request in the database. The unauthorized user does not attempt to upload a real file, but rather includes in their request a "comment" to be associated with the file upload. The server takes the comment, encrypts it using the encryption key, and stores it in the database.[170]

1093. The result is an entry in the MOVEit Transfer database for a paused file upload containing the encrypted comment[171]:

[166] *Id.*

[167] *Id.*

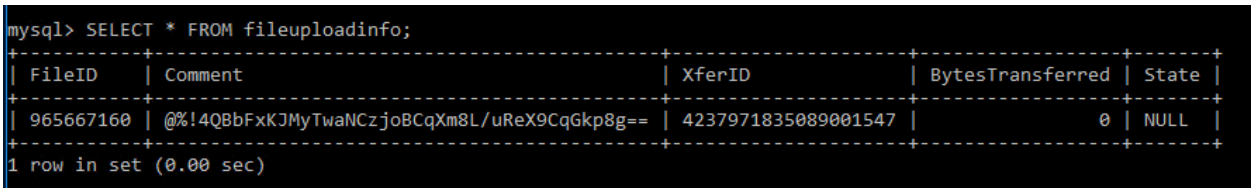
[168] *Id.*

[169] *Id.*

[170] *Id.*

[171] *Id.*

Figure 4



1094. The unauthorized user then uses SQL injection to move the value in the "Comment" column to the "State" column.[172]

1095. The unauthorized user can make the "Comment" a serialized malicious program, which can be accomplished easily with a tool such as YSoSerial.Net.[173]

1096. When the unauthorized user prompts the server to resume the file upload, the server decrypts the "State" column—now containing the unauthorized user's serialized malicious program—into a .NET BinaryFormatter type and performs the function Deserialize on it.[174]

1097. Because of the way that the BinaryFormatter.Deserialize function works, as outlined above, this action effectively executes the malicious code that was written into the "State" column.[175]

1098. The unauthorized user's malicious code is executed as a .NET program running at the root level rather than by the SQL engine running only within the database. The code therefore has access to the same context as a .NET program, *i.e.*, the entire server and all files on the server, not just the MOVEit Transfer software.[176]

---

[172] *Id.*

[173] *Id.*

[174] *Id.*

[175] *Id.*

[176] *Id.*; *Deserialization risks in use of BinaryFormatter and related types*, Microsoft Build: Learn .NET (Apr. 4, 2023), https://learn.microsoft.com/en-us/dotnet/standard/serialization/binary formatter-security-guide.

1099. CL0P used the SQL injection and BinaryFormatter.Deserialize vulnerabilities to install a malicious web shell called LEMURLOOT on MOVEit Transfer servers.[177]

1100. A web shell is a program that allows a user to execute commands on a web server without having physical access to it.[178]

1101. LEMURLOOT was written specifically to compromise MOVEit Transfer servers, evidenced by its use of MOVEit Transfer-specific code libraries—*i.e.*, commands that can be sent to the MOVEit Transfer software to perform certain functions.[179]

1102. LEMURLOOT "authenticates incoming connections via a hard-coded password" to ensure that only CL0P can access the LEMURLOOT web shell. [180]

1103. LEMURLOOT "can run commands that will download files from the MOVEit Transfer system, extract its Azure system settings, retrieve detailed record information, create and insert a particular user, or delete this same user."[181]

1104. LEMURLOOT can also access files containing server credentials, such as Azure Storage Blob information.[182]

---

[177] Nader Zaveri et al., *Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft*, Mandiant: Blog (Apr. 3, 2024), https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft.

[178] Cybersecurity & Infrastructure Sec. Agency (CISA), *Compromised Web Servers and Web Shells - Threat Awareness and Guidance*, Alert: TA15-314A (Aug. 9, 2017), https://www.cisa.gov/news-events/alerts/2015/11/10/compromised-web-servers-and-web-shells-threat-awareness-and-guidance.

[179] *#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, Cybersecurity & Infrastructure Sec. Agency (CISA) (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[180] Nader Zaveri et al., *Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft*, Mandiant: Blog (Apr. 3, 2024), https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft.

[181] *Id.*

[182] *Id.*

1105. Even though MOVEit Transfer encrypts files in transit and at rest, MOVEit Transfer does not store its encryption keys securely. Rather, MOVEit Transfer software is designed to simply retrieve an encryption key and decrypt files when prompted by an authenticated user—even a malicious user like LEMURLOOT.[183]

1106. Therefore, when LEMURLOOT is installed on a MOVEit Transfer server, it can leverage the MOVEit Transfer software to decrypt the stored files without additionally having to obtain the encryption key.[184]

1107. Accordingly, the defective design of the MOVEit Transfer software allowed CL0P to simultaneously access, decrypt and exfiltrate data, essentially giving CL0P unfettered access to unencrypted and unredacted data.

1108. LEMURLOOT was given the file name "human2.aspx" to mimic the file name of the legitimate MOVEit Transfer file "human.aspx" and avoid detection.[185]

1109. Below is an example log detailing the server requests performed in the attacks, ultimately leading to successful access to the LEMURLOOT web shell at "human2.aspx"[186]:

[183] Steven Coffey, Josh Mitchell, & Dan Cox, *MOVEit Vulnerability Investigations Uncover Additional Exfiltration Method*, Kroll (July 24, 2024), https://www.kroll.com/en/insights/publications/cyber/moveit-vulnerability-investigations-uncover-additional-exfiltration-method.

[184] Tr33, Understanding CVE-2023-34362: A critical MOVEit Transfer vulnerability, Hack The Box (Oct. 16, 2023), https://www.hackthebox.com/blog/cve-2023-34362-explained.

[185] Dan Goodin, *Mass exploitation of critical MOVEit flaw is ransacking orgs big and small*, Ars Technica (June 5, 2023, 10:05 PM) https://arstechnica.com/information-technology/2023/06/mass-exploitation-of-critical-moveit-flaw-is-ransacking-orgs-big-and-small/.

[186] Scott Downie et al., *Clop Ransomware Likely Sitting on MOVEit Transfer Vulnerability (CVE-2023-34362) Since 2021*, Kroll (Jun. 8, 2023), https://www.kroll.com/en/insights/publications/cyber/clop-ransomware-moveit-transfer-vulnerability-cve-2023-34362.

Figure 5

1110. Data theft can occur within minutes of deployment of the web shell.[187]

1111. Though MOVEit Transfer's SQL injection vulnerability was exploited to provide unauthorized users with administrative permissions within the MOVEit Transfer software, these permissions would still limit the user to the capabilities of the MOVEit Transfer software—*i.e.*, the user would still only be able to access and download files in the manner that the MOVEit Transfer software is designed, which could be slow and tedious. The addition of the LEMURLOOT web shell, by exploiting the BinaryFormatter.Deserialize vulnerability, substantially increased the speed and efficiency of the attacks because the web shell could decrypt, compress, and bulk download files directly from the server, without having to work within the MOVEit Transfer software.[188]

[187] Nader Zaveri et al., *Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft*, Mandiant: Blog (Apr. 3, 2024), https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft.

[188] *Id.*

1112. All versions of MOVEit Transfer are subject to these critical vulnerabilities—which have long been understood and documented—confirming that the vulnerabilities existed in MOVEit Transfer for years without being discovered or fixed in subsequent versions.[189]

1113. MOVEit versions as old as 2020 (and possibly even earlier) were ultimately patched to fix these critical vulnerabilities after the Data Breach, further confirming that Progress supports and permits clients to use versions of the software that are many years old and were developed with these vulnerabilities.[190]

1114. These vulnerabilities and attack vectors have been widely reported and tested by multiple third parties, further verifying that the Data Breach occurred in substantially the same manner as detailed above.[191]

4. Zero-Day.

1115. MOVEit Transfer, as a popular, highly available, and widely-distributed software installed on individual customers' servers—and "thus not easily patched"—and accessible over the Internet, presented a unique opportunity for hackers because public-facing MOVEit Transfer server web applications can be found easily by searching the Internet, and numerous MOVEit

[189] *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)*, Progress: Community (June 16, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023.

[190] *Id.*

[191] Nader Zaveri et al., *Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft*, Mandiant: Blog (Apr. 3, 2024), https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft; Zach Hanley, *MOVEit Transfer CVE-2023-34362 Deep Dive and Indicators of Compromise*, Horizon3.ai: Attack Blogs (June 9, 2023), https://www.horizon3.ai/attack-research/attack-blogs/moveit-transfer-cve-2023-34362-deep-dive-and-indicators-of-compromise/; John Hammond, *MOVEit Transfer Critical Vulnerability CVE-2023-34362 Rapid Response*, Huntress: Blog (June 1, 2023), https://www.huntress.com/blog/moveit-transfer-critical-vulnerability-rapid-response.

Transfer customers could be attacked simultaneously—and automatically—with the same exact strategy.[192]

1116. Because MOVEit Transfer software is installed on customers' servers rather than Progress servers, CL0P scanned the Internet looking for servers with publicly accessible MOVEit Transfer login pages, denoted by a page called "human.aspx."[193]

1117. Traffic from known CL0P IP addresses began scanning the Internet for MOVEit Transfer login pages, attempting to discover vulnerable MOVEit Transfer installations, as early as July 2021.[194]

1118. CL0P had therefore been developing this strategy and planning their targets since 2021, ready to inflict the maximum amount of damage in a short amount of time.[195]

1119. Using a strategy similar to that outlined above, CL0P was able to exploit vulnerabilities in the MOVEit Transfer software to gain access to each server's files without detection.[196]

---

[192] Joe Slowik, *Move It on Over: Reflecting on the MOVEit Exploitation*, Huntress: Blog (Jul. 7, 2023), https://www.huntress.com/blog/move-it-on-over-reflecting-on-the-moveit-exploitation.

[193] Matthew Remacle, *Progress' MOVEit Transfer Critical Vulnerability: CVE-2023-34362*, GreyNoise: Blog (June 1, 2023), https://www.greynoise.io/blog/progress-moveit-transfer-critical-vulnerability.

[194] Scott Downie et al., *Clop Ransomware Likely Sitting on MOVEit Transfer Vulnerability (CVE-2023-34362) Since 2021*, Kroll (Jun. 8, 2023), https://www.kroll.com/en/insights/publications/cyber/clop-ransomware-moveit-transfer-vulnerability-cve-2023-34362.

[195] *Id.*

[196] Nader Zaveri et al., *Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft*, Mandiant: Blog (Apr. 3, 2024), https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft.

1120. It is not known when CL0P began deploying this strategy, but the earliest publicly available evidence shows that CL0P began installing LEMURLOOT on MOVEit Transfer servers by May 27, 2023.[197]

1121. May 27, 2023, coincided with Memorial Day weekend, consistent with a common strategy employed by hackers to launch attacks on holiday weekends when victims may be unable to respond.[198]

1122. Because the MOVEit Transfer software was not designed to discover or defend against this type of attack, it initially went undetected.[199]

1123. Such attacks are called "zero-day" attacks because the specific flaw is exploited before the developer is aware of it—*i.e.*, the developer has had zero days to release a patch.[200]

1124. Because data theft can occur within minutes of deployment of LEMURLOOT, CL0P was able to simultaneously attack thousands of MOVEit Transfer servers and steal troves of data in a relatively short time before detection.[201]

---

[197] Id.

[198] Scott Downie et al., *Clop Ransomware Likely Sitting on MOVEit Transfer Vulnerability (CVE-2023-34362) Since 2021*, Kroll (Jun. 8, 2023), https://www.kroll.com/en/insights/publications/cyber/clop-ransomware-moveit-transfer-vulnerability-cve-2023-34362.

[199] Nader Zaveri et al., *Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft*, Mandiant: Blog (Apr. 3, 2024), https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft.

[200] *What is a Zero-day Attack? - Definition and Explanation*, Kaspersky, https://usa.kaspersky.com/resource-center/definitions/zero-day-exploit (last visited Nov. 26, 2024).

[201] Nader Zaveri et al., *Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft*, Mandiant: Blog (Apr. 3, 2024), https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft.

5. Discovery of the Data Breach.

1125. On May 28, 2023, "the MOVEit technical support team received initial customer calls indicating suspicious activity."[202]

1126. A malicious "staged exploit" was discovered and removed from three MOVEit Cloud clusters on May 30, 2023.[203]

1127. MOVEit Cloud was temporarily shut down on May 30 and May 31, 2023;[204] MOVEit Cloud service was restored on May 31, 2023.[205]

1128. On May 31, 2023, Progress announced the discovery of an "SQL injection vulnerability . . . in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database."[206]

1129. Progress found that, "depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database and execute SQL statements that alter or delete database elements."[207]

1130. Progress found that the vulnerability was "exploited in the wild in May and June 2023."[208]

---

[202] *Status of the May 2023 security vulnerability and defensive outage of MOVEit Cloud*, Progress: Community (June 1, 2023), https://community.progress.com/s/article/MOVEit-Cloud-Info-Regarding-Critical-Vulnerability-May-2023.

[203] *Id.*

[204] *Id.*

[205] *Id.*

[206] *Id.*

[207] *Id.*

[208] *Id.*

1131. The vulnerability affected "[a]ll MOVEit Transfer versions."[209]

1132. The Data Breach was further publicized on June 5, 2023, when multiple companies began coming forward to announce that their MOVEit Transfer servers were compromised.[210]

1133. Signs of a breach in a customer's MOVEit Transfer database are evidenced by unauthorized entries in the "userexternaltokens," "trustedexternaltokenproviders," and "hostpermits" tables whereby the sysadmin was obtained, as well as log entries for the endpoints that the unauthorized users utilized[211]:

a. <InstallDir>/Logs/DMZ_WebApi.log when requests are made to /api/v1/ endpoints

b. <InstallDir>/Logs/DMZ_WEB.log when requests are made to /guestaccess.aspx and relayed messages to /machine2.aspx

c. <InstallDir>/Logs/DMZ_ISAPI.log when requests are made to /moveitisapi/moveitisapi.dll?action=m2

1134. Though a malicious "staged exploit" was discovered on MOVEit Cloud clusters, Progress reported that there was no evidence that the exploit was activated or that MOVEit Cloud data was compromised.[212]

---

[209] *Id.*

[210] Matt Kapko, *Worries mount for MOVEit vulnerability, as likelihood of compromise expands*, Cybersecurity Drive (June 5, 2023), https://www.cybersecuritydive.com/news/moveit-vulnerability-worries-mount/652035/.

[211] Nader Zaveri et al., *Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft*, Mandiant: Blog (Apr. 3, 2024), https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft.

[212] *Status of the May 2023 security vulnerability and defensive outage of MOVEit Cloud*, Progress: Community (June 1, 2023), https://community.progress.com/s/article/MOVEit-Cloud-Info-Regarding-Critical-Vulnerability-May-2023.

1135. Progress has conceded in these proceedings that MOVEit Cloud utilizes the same code that was subject to the same vulnerabilities as MOVEit Transfer and has acknowledged the same remedial strategy was used on both.

E. Progress's May 31 patch that came too late.

1. Mitigating and patching the MOVEit vulnerabilities.

1136. On May 31, 2023, Progress published its finding of an "SQL injection vulnerability . . . in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database and execute SQL statements that alter or delete database elements."[213]

1137. The vulnerability was given the unique identifier CVE-2023-34362 in the National Vulnerability Database maintained by the United States National Institute of Standards and Technology ("NIST").[214]The National Institute of Standards and Technology utilizes the Common Vulnerability Scoring System and has a calculator for establishing criticality scores.[215] The common vulnerability scoring system (CVSS) is widely used to classify vulnerabilities. This is an open industry standard that allows for the scoring of vulnerabilities based on severity. The full

[213] *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)*, Progress: Community (June 16, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023.

[214] NIST, *Progress MOVEit Transfer SQL Injection Vulnerability (CVE-2023-34362) Detail*, Nat'l Vulnerability Database (June 23, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-34362.

[215] *Common Vulnerability Scoring System Calculator*, NIST, https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator (last visited Nov. 26, 2024).

specification can be found online.[216] There are three groups of metrics: base, temporal, and environmental. The base group describes the basic characteristics of the vulnerability that are not determined by time (temporal) or environment. The metrics in this group are Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, Confidentiality Impact, Integrity Impact, and Availability Impact. The Temporal Metric Group has three metrics: Exploit Code Maturity, Remediation Level, and Report Confidence. The Environmental Metric Group has four metrics: Modified Base Metrics, Confidentiality Requirement, Integrity Requirement, and Availability Requirement.

1138. The vulnerability was given a severity rating under the Common Vulnerability Scoring System of 9.8 out of 10, signifying that the vulnerability is near the highest level of severity, or "critical."[217]

1139. The vulnerability was marked with a Common Weakness Enumeration code CWE-89, for "Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')."[218]

1140. Progress recommended the following steps to mitigate the damage caused by the vulnerability until a patch could be installed[219]:

---

[216] *Common Vulnerability Scoring System version 4.0: Specification Document*, First, https://www.first.org/cvss/specification-document (last visited Nov. 26, 2024).

[217] *Id.*

[218] NIST, *CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (CVE-2023-42660) Detail*, Nat'l Vulnerability Database (Aug. 22, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-42660; NIST, *CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (CVE-2023-40043) Detail*, Nat'l Vulnerability Database (Aug. 22, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-40043.

[219] *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)*, Progress: Community (June 16, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023.

a. "Disable all HTTP and HTTPs traffic to your MOVEit Transfer environment"

b. "Delete Unauthorized Files and User Accounts"

c. "Reset service account credentials for affected systems and MOVEit Service Account"

1141. Progress published a patch on May 31, 2023, with updated code that Progress claims will prevent further SQL injection attacks and remote code execution as outlined above, stating[220]:

> Progress has discovered a vulnerability in MOVEit Transfer that could lead to escalated privileges and potential unauthorized access to the environment. If you are a MOVEit Transfer customer, it is extremely important that you take immediate action as noted below in order to help protect your MOVEit Transfer environment.

1142. Cybersecurity firm Huntress investigated the CVE-2023-34362 attack vector and discovered another SQL injection attack vector, which was assigned CVE-2023-35036.[221]

1143. Progress published another patch on June 9, 2023, for CVE-2023-35036, again with the CWE-89 SQL injection vulnerability, stating[222]:

> SQL Injection (CVE-2023-35036) In Progress MOVEit Transfer versions released before 2021.0.7 (13.0.7), 2021.1.5 (13.1.5), 2022.0.5 (14.0.5), 2022.1.6 (14.1.6), 2023.0.2 (15.0.2), multiple SQL injection vulnerabilities have been identified in the MOVEit Transfer web application that could allow an un-authenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint which could result in modification

[220] Dan Goodin, *Mass exploitation of critical MOVEit flaw is ransacking orgs big and small*, Ars Technica (June 5, 2023, 10:05 PM) https://arstechnica.com/information-technology/2023/06/mass-exploitation-of-critical-moveit-flaw-is-ransacking-orgs-big-and-small/.

[221] John Hammond, *MOVEit Transfer Critical Vulnerability CVE-2023-34362 Rapid Response*, Huntress: Blog (June 1, 2023), https://www.huntress.com/blog/moveit-transfer-critical-vulnerability-rapid-response.

[222] *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)*, Progress: Community (June 16, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023.

> and disclosure of MOVEit database content. All versions of MOVEit Transfer are affected by this vulnerability. Patches for this vulnerability are available for supported versions and are listed in the Recommended Remediation section.

1144. Progress published another patch on June 15, 2023, for yet another newly discovered attack vector, CVE-2023-35708, again with the CWE-89 SQL injection vulnerability, stating[223]:

> Progress has discovered a vulnerability in MOVEit Transfer that could lead to escalated privileges and potential unauthorized access to the environment. If you are a MOVEit Transfer customer, it is extremely important that you take immediate action as noted below in order to help protect your MOVEit Transfer environment. In Progress MOVEit Transfer versions released before 2021.0.8 (13.0.8), 2021.1.6 (13.1.6), 2022.0.6 (14.0.6), 2022.1.7 (14.1.7), 2023.0.3 (15.0.3), a SQL injection vulnerability has been identified in the MOVEit Transfer web application that could allow an un-authenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint which could result in modification and disclosure of MOVEit database content.

1145. On July 6, 2023, Progress released another service pack containing patches for three more newly discovered vulnerabilities in MOVEit Transfer[224]—two involving SQL injection (CWE-89)[225] and one involving Improper Handling of Exceptional Conditions (CWE-755).[226]

---

[223] *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)*, Progress: Community (June 16, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023.

[224] *MOVEit Transfer Service Pack – (July 2023)*, Progress: Community (July 6, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-July-2023.

[225] NIST, *CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (CVE-2023-36932) Detail*, Nat'l Vulnerability Database (July 12, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-36932; NIST, *CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (CVE-2023-36934) Detail*, Nat'l Vulnerability Database (July 10, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-36934.

[226] NIST, *CWE-755 Improper Handling of Exceptional Conditions (CVE-2023-36933) Detail*, Nat'l Vulnerability Database (July 12, 2023), https://nvd.nist.gov/vuln/detail/CVE-2023-36933.

1146. On September 20, 2023, Progress released another service pack containing patches for three more newly discovered vulnerabilities in MOVEit Transfer[227]—two involving SQL injection (CWE-89)[228] and one involving Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CWE-79).[229]

1147. On November 29, 2023, Progress released another service pack containing patches for two more newly discovered vulnerabilities in MOVEit Transfer[230]—one involving Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CWE-79)[231] and one involving Improper Privilege Management (CWE-269).[232]

[227] *MOVEit Transfer Service Pack – (July 2023)*, Progress: Community (July 6, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-July-2023.

[228] NIST, *CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (CVE-2023-42660) Detail*, Nat'l Vulnerability Database, https://nvd.nist.gov/vuln/detail/CVE-2023-42660 (last updated Nov. 21, 2024); NIST, *CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (CVE-2023-40043) Detail*, Nat'l Vulnerability Database, https://nvd.nist.gov/vuln/detail/CVE-2023-40043 (last updated Nov. 21, 2024).

[229] NIST, *CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CVE-2023-42656) Detail*, Nat'l Vulnerability Database, https://nvd.nist.gov/vuln/detail/CVE-2023-42656 (last updated Nov. 21, 2024).

[230] *MOVEit Transfer Service Pack - (Nov. 2023)*, Progress: Community (Nov. 29, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-November-2023.

[231] NIST, *CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CVE-2023-6217) Detail*, Nat'l Vulnerability Database, https://nvd.nist.gov/vuln/detail/CVE-2023-6217 (last updated Nov. 21, 2024).

[232] NIST, *CWE-269 Improper Privilege Management (CVE-2023-6218) Detail*, Nat'l Vulnerability Database, https://nvd.nist.gov/vuln/detail/CVE-2023-6218 (last updated Nov. 21, 2024).

1148. On January 17, 2024, Progress released another service pack containing a patch for another newly discovered vulnerability in MOVEit Transfer[233] involving Improper Input Validation (CWE-20).[234]

1149. On March 21, 2024, Progress released another service pack containing a patch for another newly discovered vulnerability in MOVEit Transfer[235] involving Insufficient Logging (CWE-778).[236]

1150. Patches are only effective after customers are informed about them and install them, as "[c]ybercriminals often probe systems and networks to see if they are out of date and missing a security patch."[237]

1151. Since the discovery of the MOVEit Transfer SQL injection vulnerabilities, Progress has continued to be plagued with critical vulnerabilities found in its other software products as it reviews outdated and insecure code[238]:

> **WS_FTP Server Critical Vulnerability (September 2023)**
>
> The WS_FTP team recently discovered vulnerabilities in the WS_FTP Server Ad hoc Transfer Module and in the WS_FTP

[233] *MOVEit Transfer Service Pack – (Jan. 2024)*, Progress: Community (Jan. 17, 2024), https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-January-2024.

[234] NIST, *CWE-20 Improper Input Validation & NVD-CWE-Info Insufficient Information (CVE-2024-0396) Detail*, Nat'l Vulnerability Database, https://nvd.nist.gov/vuln/detail/CVE-2024-0396 (last updated Nov. 21, 2024).

[235] *MOVEit Transfer Service Pack (March 2024)*, Progress: Community (Mar. 21, 2024), https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-March-2024.

[236] NIST, *CWE-778 Insufficient Logging (CVE-2024-2291) Detail*, Nat'l Vulnerability Database, https://nvd.nist.gov/vuln/detail/CVE-2024-2291 (last updated Nov. 21, 2024).

[237] Arya Arun, *Cyber Security Vulnerability: Signs Your Network & Systems May Be Weak*, StickmanCyber (July 21, 2022), https://www.stickmancyber.com/cybersecurity-blog/cyber-security-vulnerability-signs-your-network-systems-may-be-weak.

[238] *Critical Alerts*, Progress: Community, https://community.progress.com/s/global-search/%40uri#t=KnowledgeBase&sort=date%20descending&f:@sfarticletypec=[Critical_Alert] (last visited Nov. 26, 2024).

Server manager interface. All versions of WS_FTP Server are affected by these vulnerabilities. We have addressed these issues and have made version-specific hotfixes available for customers to remediate them.[239]

* * *

WS_FTP Server Service Pack (November 2023)

This article contains the details of the specific updates within the WS_FTP Server November 2023 Service Pack. The Service Pack contains fixes for one newly disclosed CVE described below. Progress Software highly recommends you apply this Service Pack for product updates and security improvements. For Service Pack content, please review the Service Pack Release Notes and this knowledgebase article carefully to help you plan when it is appropriate to apply to your environments.[240]

* * *

Important Progress OpenEdge Critical Alert for Progress Application Server in OpenEdge (PASOE) - Arbitrary File Upload Vulnerability in WEB Transport

The WEB transport in PASOE has support for file uploads across all web handlers and all web handlers are affected including the built-in handlers. The expected behavior is that file upload is disabled by default since the value for the "fileUploadDirectory" property in the openedge.properties file is blank. However, this default property setting allows access to all directories for the user account that started the PASOE instance. If these directories have write permission, the system running PASOE is vulnerable to a malicious file upload on the system (Linux) or on the root drive (Windows). An attacker with the unexpected ability to upload to the system running PASOE could then launch a wider scale attack.[241]

---

[239] *WS_FTP Server Critical Vulnerability (Sept. 2023)*, Progress: Community (Oct. 20, 2023), https://community.progress.com/s/article/WS-FTP-Server-Critical-Vulnerability-September-2023.

[240] *WS_FTP Server Service Pack (Nov. 2023)*, Progress: Community (Nov. 7, 2023), https://community.progress.com/s/article/WS-FTP-Server-Service-Pack-November-2023.

[241] Important Progress OpenEdge Critical Alert for Progress Application Server in OpenEdge (PASOE) - Arbitrary File Upload Vulnerability in WEB Transport, Progress: Community (Jan. 18, 2024), https://community.progress.com/s/article/Important-Progress-OpenEdge-Critical-Alert-

* * *

> **Important Security Update for OpenEdge Authentication Gateway and AdminServer**
>
> When the OpenEdge Authentication Gateway (OEAG) is configured with an OpenEdge Domain that uses the OS local authentication provider to grant user-id and password logins on operating platforms supported by active releases of OpenEdge, a vulnerability in the authentication routines may lead to unauthorized access on attempted logins.
>
> Similarly, when an AdminServer connection is made by OpenEdge Explorer (OEE) and OpenEdge Management (OEM), it also utilizes the OS local authentication provider on supported platforms to grant user-id and password logins that may also lead to unauthorized login access.[242]

1152. These more recent critical vulnerabilities involved the following Common Weakness Enumerations, as reported by NIST, some of which are the same as the SQL injection and deserialization vulnerabilities found in MOVEit Transfer:

a. CVE-2023-40044: CWE-502 Deserialization of Untrusted Data[243]

b. CVE-2023-42657: CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')[244]

for-Progress-Application-Server-in-OpenEdge-PASOE-Arbitrary-File-Upload-Vulnerability-in-WEB-Transport.

[242] *Important Security Update for OpenEdge Authentication Gateway and AdminServer*, Progress: Community (Feb. 27, 2024), https://community.progress.com/s/article/Important-Critical-Alert-for-OpenEdge-Authentication-Gateway-and-AdminServer.

[243] NIST, *CWE*-502 *Deserialization of Untrusted Data (CVE-2023-40044) Detail*, Nat'l Vulnerability Database, https://nvd.nist.gov/vuln/detail/CVE-2023-40044 (last updated Nov. 21, 2024).

[244] NIST, *CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (CVE-2023-42657) Detail*, Nat'l Vulnerability Database, https://nvd.nist.gov/vuln/detail/CVE-2023-42657 (last updated Nov. 21, 2024).

c. CVE-2023-40045: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')[245]

d. CVE-2023-40046: CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')[246]

e. CVE-2023-40047: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')[247]

f. CVE-2023-40048: CWE-352 Cross-Site Request Forgery (CSRF)[248]

g. CVE-2022-27665: CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')[249]

h. CVE-2023-40049: CWE-200 Exposure of Sensitive Information to an Unauthorized Actor[250]

i. CVE-2023-42659: CWE-434 Unrestricted Upload of File with Dangerous Type[251]

j. CVE-2023-40051: CWE-434 Unrestricted Upload of File with Dangerous Type[252]

---

[245] *CVE-2023-40045 Detail*, NIST, https://nvd.nist.gov/vuln/detail/CVE-2023-40045 (last updated Nov. 21, 2024).

[246] *CVE-2023-40046 Detail*, NIST, https://nvd.nist.gov/vuln/detail/CVE-2023-40046 (last updated Nov. 21, 2024).

[247] *CVE-2023-40047 Detail*, NIST, https://nvd.nist.gov/vuln/detail/CVE-2023-40047 (last updated Nov. 21, 2024).

[248] *CVE-2023-40048 Detail*, NIST, https://nvd.nist.gov/vuln/detail/CVE-2023-40048 (last updated Nov. 21, 2024).

[249] *CVE-2022-27665 Detail*, NIST, https://nvd.nist.gov/vuln/detail/CVE-2022-27665 (last updated Nov. 21, 2024).

[250] *CVE-2023-40049 Detail*, NST, https://nvd.nist.gov/vuln/detail/CVE-2023-40049 (last updated No. 21, 2024).

[251] *CVE-2023-42659 Detail*, NIST, https://nvd.nist.gov/vuln/detail/CVE-2023-42659 (last updated No. 21, 2024).

[252] *CVE-2023-40051 Detail*, NIST, https://nvd.nist.gov/vuln/detail/CVE-2023-40051 (last updated Nov. 21, 2024).

k. CVE-2024-1403: CWE-305 Authentication Bypass by Primary Weakness[253]

1153. These critical vulnerabilities show that Progress continues to employ poorly written, outdated, and insecure code in its software, without updating outdated code, checking for known or newly discovered vulnerabilities, or following industry standards for software security.

1154. Progress knew or should have known about the vulnerabilities affecting MOVEit Transfer, and Progress was negligent in developing and maintaining MOVEit Transfer, because:

a. Progress did not adhere to basic, well-known industry standards for software security.

b. Progress did not review and maintain MOVEit Transfer code to ensure it was secure and met industry standards.

c. Progress allowed customers to use outdated versions of MOVEit Transfer software.

d. Progress developed and maintained MOVEit Cloud without the vulnerabilities affecting MOVEit Transfer.

2. CL0P takes responsibility and ransoms stolen data.

1155. Organizations with compromised MOVEit Transfer servers were not immediately contacted with ransom demands when the Data Breach occurred.[254]

1156. On June 4, 2023, Microsoft attributed the Data Breach "to Lace Tempest, known for ransomware operations & running the Clop extortion site. The threat actor has used similar vulnerabilities in the past to steal data & extort victims."[255]

---

[253] *CVE-2024-41403 Detail*, NIST, https://nvd.nist.gov/vuln/detail/CVE-2024-1403 (last updated Nov. 21, 2024).

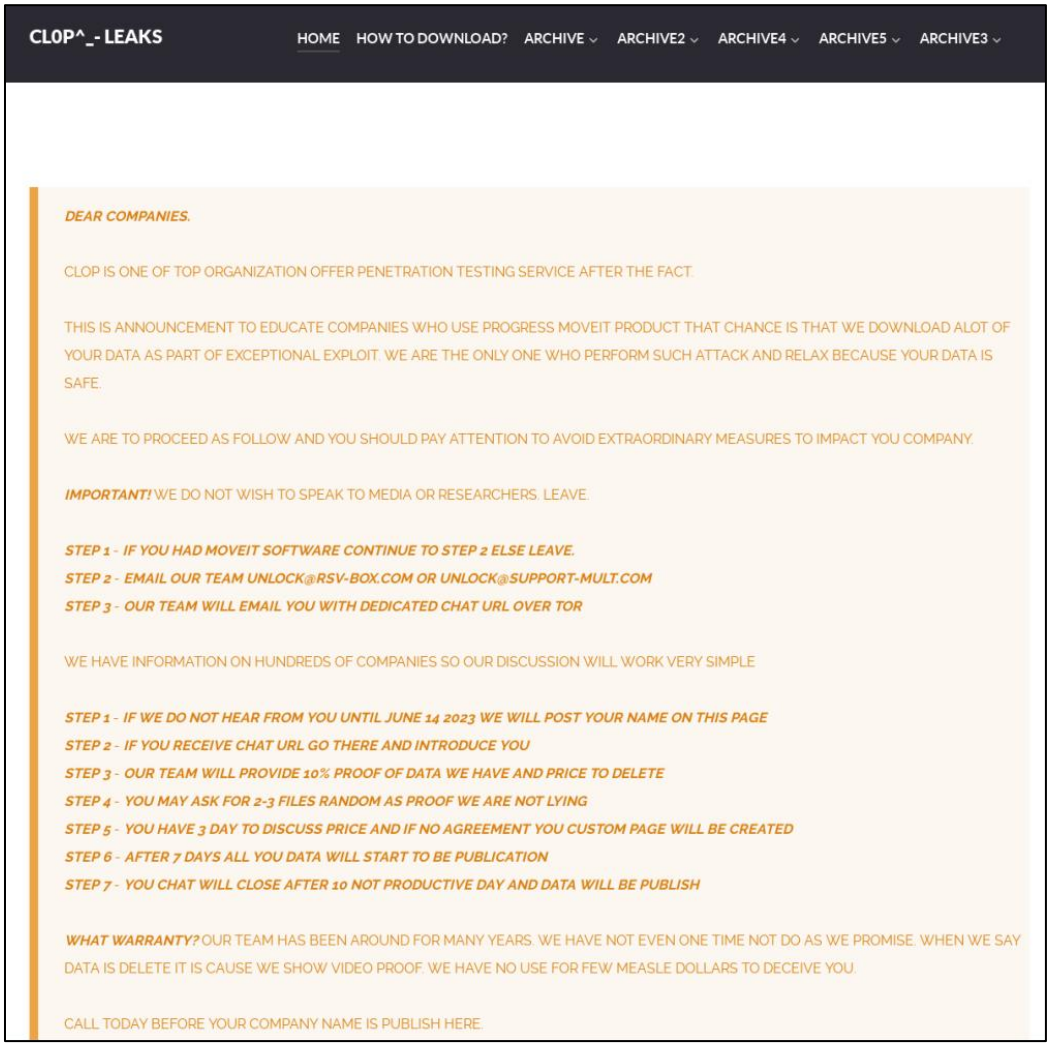
[254] Nader Zaveri et al., *Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft*, Mandiant: Blog (Apr. 3, 2024), https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft.

[255] @MsftSecIntel, Twitter (Jun. 4, 2023, 8:55 PM), https://twitter.com/MsftSecIntel/status/1665537730946670595.

1157. On June 6, 2023, after the Data Breach was publicized and a patch was rolled out, CL0P took responsibility for the Data Breach and threatened to post stolen data online unless the compromised organizations paid a ransom.[256]

1158. A CL0P ransom note is reproduced below[257]:

Figure 6



[256] Nader Zaveri et al., *Zero-Day Vulnerability in MOVEit Transfer Exploited for Data Theft*, Mandiant: Blog (Apr. 3, 2024), https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft.

[257] Satnam Narang, *CVE-2023-34362: MOVEIt Transfer Critical Zero-Day Vulnerability Exploited in the Wild*, Tenable: Blog (Jun. 2, 2023), https://www.tenable.com/blog/cve-2023-34362-moveit-transfer-critical-zero-day-vulnerability-exploited-in-the-wild.

1159. CL0P threatened to name and publish leaked data of any organizations that did not respond to their ransom demands.[258]

1160. The deadline for CL0P's ransom demands expired on June 14, 2023.[259]

1161. On June 14, 2023, CL0P released a list of 12 organizations that had data compromised in the Data Breach on their dark website >_CLOP^_-LEAKS.[260]

1162. CL0P continued to update this published list and leak terabytes of information, presumably as organizations either rejected or gave into CL0P's ransom demands.[261]

1163. By July 28, 2023, CL0P had named over 250 organizations on its dark website in relation to the Data Breach.[262]

1164. By December 20, 2023, over 2,600 organizations had been named as victims of the Data Breach.[263]

1165. Research by Censys found[264]:

- 30.86% of the hosts running MOVEit are in the financial services industry, 15.96% in healthcare, 8.82% in information technology, and 7.56% in government and military.

---

[258] Riam Kim-Mcleod, *Clop Leaks: First Wave of Victims Named*, ReliaQuest: Blog (July 28, 2023, 10:00 AM), https://www.reliaquest.com/blog/clop-leaks-first-victims/.

[259] Matt Kapko, *Worries mount for MOVEit vulnerability, as likelihood of compromise expands*, Cybersecurity Drive (June 5, 2023), https://www.cybersecuritydive.com/news/moveit-vulnerability-worries-mount/652035/.

[260] Riam Kim-Mcleod, *Clop Leaks: First Wave of Victims Named*, ReliaQuest: Blog (July 28, 2023, 10:00 AM), https://www.reliaquest.com/blog/clop-leaks-first-victims/.

[261] *Id.*

[262] *Id.*

[263] Bert Kondruss, *MOVEit hack victim list*, Kon Briefing, https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html (last updated Dec. 20, 2023).

[264] *MOVEit: an Industry Analysis*, Censys (June 13, 2023), https://censys.com/moveit-an-industry-analysis/.

- 29% of the companies we observed have over 10,000 employees, indicating that this service is used in a variety of large organizations.

- Companies based in the United States account for a significant majority, comprising 69%, of MOVEit hosts.

1166. The United States Cybersecurity and Infrastructure Security Agency ("CISA") offered a bounty up to $10 million for information linking CL0P or other malicious cyber actors targeting United States critical infrastructure to foreign governments.[265]

II. The Effects of the Data Breach.

1167. The effects of the Data Breach are devastating.

1168. Due to the sensitive nature of the information moved using the MOVEit products, the Plaintiffs and Class Members have suffered significant exposure and are now at an elevated risk for identity theft and fraud, while many have already experienced significant fraud, identity theft, and other related issues.

1169. The kinds of information exposed in the Data Breach provide hackers and cybercriminals a wealth of opportunities for committing additional crimes and harming Plaintiffs and Class Members even further.

1170. Fraud and identity theft will continue to happen, through the buying, selling, ransoming, and continued exploitation of the personal information, financial information, personal health information, and other sensitive information exposed in this far-reaching Data Breach.

[265] @RFJ_USA, Twitter (Jun. 16, 2023), https://twitter.com/RFJ_USA/status/1669740545403437056.

A. The MOVEit software was used to transfer PII and PHI.

1171. The MOVEit software was commonly used by healthcare companies, healthcare benefits providers, hospital systems, and other health-related entities, to move PHI.[266]

1172. In addition, banking and financial institutions, pension benefit plans, health insurers, colleges and universities, state governments and local municipalities, biotech companies, charter schools, credit unions, emergency services corporations, IT services companies, marketing companies, social service providers, software and technology companies, and many, many more were breached through the MOVEit Transfer and Cloud technologies.[267]

1173. In excess of 2,600 different, individual entities were breached via the MOVEit vulnerabilities in the United States alone.[268]

1174. Progress's MOVEit technology, both MOVEit Transfer and MOVEit Cloud, were primarily used by Defendants as a secure file-transfer tool.[269]

1175. By January 1, 2024, over 93 million individual records had been exposed and the numbers are only growing.

1176. The sensitive information moved by these tools was the kind of information each Class Member expected would be treated with care and kept confidential, including, but not limited to:

---

[266] Bert Kondruss, *MOVEit hack victim list*, Kon Briefing, https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html (last updated Dec. 20, 2023).

[267] *Id.*

[268] *Id.*

[269] *MOVEit® Transfer*, Progress MOVEit https://webobjects2.cdw.com/is/content/CDW/cdw/on-domain-cdw/brands/progress/progress-moveit-transfer-datasheet0323.pdf (last visited Nov. 26, 2024).

i. Names[270]

ii. Dates of birth[271]

iii. Addresses[272]

iv. Telephone numbers[273]

v. Social Security numbers[274]

vi. Subscriber/member ID numbers[275]

vii. Driver's License numbers[276]

viii. State Identification numbers[277]

ix. Policy Numbers[278]

x. Group Numbers[279]

xi. Claim Numbers[280]

xii. Medical history and diagnoses[281]

---

[270] *CMS Notifies Additional Individuals Potentially Impacted by MOVEit Data Breach*, CMS.gov (Nov. 16, 2023), https://www.cms.gov/newsroom/press-releases/cms-notifies-additional-individuals-potentially-impacted-moveit-data-breach.

[271] *Id.*

[272] *Id.*

[273] *Id.*

[274] *Id.*

[275] *Id.*

[276] *Id.*

[277] *Id.*

[278] *Id.*

[279] *Id.*

[280] *Id.*

[281] *Id.*

xiii. Medical bills and claims data[282]

xiv. Financial account numbers[283]

xv. Routing/ABA numbers[284]

xvi. Pension benefit account numbers[285]

xvii. Health insurance ID numbers[286]

xviii. Health insurance claims numbers[287] and

xix. Many other kinds of Private Information.

1177. In each case consolidated in this MDL, the MOVEit server on which Defendants kept Plaintiffs' and Class Members' Private Information was compromised, leading to the exposure of the kinds of information identified above.

1178. While various Defendants used MOVEit servers to move different kinds of Private Information, each and every Defendant used the same MOVEit products to move information of high value and sensitivity.

---

[282] *Id.*

[283] Paulina Okunytė, *Kearny Bank admits clients' financial data exposed in MOVEit breach*, cybernews (Nov. 15, 2023, 12:53 PM), https://cybernews.com/news/kearny-bank-moveit-data-breach/.

[284] Carly Page, *More organizations confirm MOVEit-related breaches as hackers claim to publish stolen data*, TechCrunch (July 6, 2023, 7:40 AM), https://techcrunch.com/2023/07/06/more-organizations-confirm-moveit-related-breaches-as-hackers-claim-to-publish-stolen-data/.

[285] *CMS Notifies Additional Individuals Potentially Impacted by MOVEit Data Breach*, CMS.gov (Nov. 16, 2023), https://www.cms.gov/newsroom/press-releases/cms-notifies-additional-individuals-potentially-impacted-moveit-data-breach.

[286] *Id.*

[287] *Id.*

B. The dark web is used by cybercriminals to share and sell Private Information.

1179. The dark web is a part of the World Wide Web that is not accessible through traditional internet browsers. The term "dark web" is used to distinguish from the "clear web," the part of the World Wide Web that is readily accessible through traditional internet browsers. The dark web is accessed through The Onion Router ("Tor"), a privacy-focused communication system designed to enable anonymous internet browsing. It achieves this by routing web traffic through multiple volunteer-operated servers (relays), encrypting data at each step to ensure that both the user's location and browsing activity are difficult to trace. Tor uses a technique called "onion routing," where data is encrypted in layers like an onion. Each relay in the network peels away a layer of encryption before passing the data to the next relay. This ensures that no single relay knows both the origin and destination of the data.

1180. Tor is based on an earlier protocol developed by the U.S. Navy, specifically for military applications. The basic concepts for onion routing were developed at the U.S. Naval Research Laboratory in the mid-1990s and later refined by the Defense Advanced Research Projects Agency ("DARPA") with the goal of providing secure intelligence communication online.[288]

1181. When using Tor, a user's IP address is masked, and their internet traffic is routed through a series of relays before reaching the destination.[289] This makes it difficult for websites,

[288] Kyle Swan, *The Origins of Tor*, 1 GEO. L. TECH. REV. 110 (2016)

[289] Massimo Bernaschi, et al., *Onion under Microscope: An in-depth analysis of the Tor network*, ads (Jan. 2021), https://ui.adsabs.harvard.edu/abs/2021arXiv210108194B/abstract.

internet service providers, or third parties to track the user's real IP address or browsing activity.[290] One can access the Tor network using a Tor browser, which is a free modified version of the Mozilla Firefox browser.[291]

1182. This process of onion routing makes for a level of anonymity that is not readily available on traditional web sites.[292] While one can utilize a fake identity on a clear web site, the website may track the user's IP address, thus revealing who the user is. Onion routing makes the entire communication process anonymous.

1183. Websites accessible only via Tor have addresses that end in ".onion." For example, the address http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/ is a popular dark web search engine. These sites can only be accessed via the Tor browser.

1184. The dark web poses significant challenges to cyber security professionals and law enforcement agencies. The dark web is legal to access and operate, and it has some legitimate applications and sites. But its hidden nature and employment of multi-level encryption make detecting and monitoring illegal activity difficult. Unlike the clear web, dark web sites do not advertise their existence.

---

[290] Dimitris Simos, et al., *On Combinatorial Security Testing for the Tor Anonymity Network Client*, NIST (Apr. 7, 2024), https://www.nist.gov/publications/combinatorial-security-testing-tor-anonymity-network-client.

[291] *Download Tor Browser*, Tor, https://www.torproject.org/download/ (last visited Nov. 26, 2024).

[292] *See* Ben Collier, *Tor From the Dark Web to the Future of Privacy*, MIT Press Direct, https://direct.mit.edu/books/oa-monograph/5761/TorFrom-the-Dark-Web-to-the-Future-of-Privacy (last visited Nov. 26, 2024).

1185. Some dark web sites are simply places for people who wish to avoid tracking while browsing the World Wide Web.[293] However, the anonymity of the dark web has led to the creation of a number of markets and forums which traffic in illegal merchandise and content, including stolen Private Information.[294]

1186. Once stolen Private Information is posted on the dark web, it will most likely be distributed to multiple different groups and individuals, each of which can use that information for fraud and identity theft.[295]

1187. This data lifecycle has also been confirmed with experiments. In 2015, researchers at BitGlass created a list of 1,568 phony names, Social Security numbers, credit card numbers, addresses, and phone numbers, rolled them in an Excel spreadsheet, and then "watermarked" it with their code that silently tracks any access to the file.[296] The data was quickly spread across five continents: North America, Asia, Europe, Africa, and South America. In the end, it was downloaded by 47 different parties. It was mainly downloaded by users in Nigeria, Russia, and

[293] Thomas J. Holt, *Open, Deep, and Dark: Differentiating the Parts of the Internet Used For Cybercrime*, Mich. State Univ., https://cj.msu.edu/_assets/pdfs/cina/CINA-White_Papers-Holt_Open_Deep_Dark.PDF (last visited Nov. 26, 2024).

[294] *Crime and the Deep Web*, Stevenson Univ., https://www.stevenson.edu/online/about-us/news/crime-deep-web/ (last visited Nov. 26, 2024); *Defending Against Malicious Cyber Activity Originating from Tor*, CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-183a (last updated Aug. 2, 2021).

[295] *The Dark Web and Cybercrime*, HHS (July 23, 2020), https://www.hhs.gov/sites/default/files/dark-web-and-cybercrime.pdf

[296] Kelly Jackson Higgins, *What Happens When Personal Information Hits The Dark Web*, DARKREADING (Apr. 7, 2015), https://www.darkreading.com/cyberattacks-data-breaches/what-happens-when-personal-information-hits-the-dark-web; Kristin Finklea, *Dark Web*, Nat'l Sec. Archive (July 7, 2015), https://nsarchive.gwu.edu/media/21394/ocr; *Dark Web*, Congressional Research Service, https://crsreports.congress.gov/product/pdf/R/R44101 (last updated Mar. 10, 2017).

Brazil, with the most activity coming from Nigeria and Russia.[297] This experiment demonstrated that data released on the dark web will quickly spread around the world.

C. Private Information of millions of individuals were exposed to CL0P and later published to the dark and clear web.

1188. Prior to the Data Breach, CL0P was known for using the "double extortion" tactic of stealing and encrypting victim data, refusing to restore victim access, and publishing exfiltrated data on the dark web via the CL0P^_-LEAKS website.[298]

1189. After exploiting the zero-day SQL vulnerability in the MOVEit software, CL0P began a campaign of contacting Defendants in this case, setting deadlines designed to extract payments in exchange for promises that the stolen information would not be published. [299]

1190. After gaining access to Defendants' systems, CL0P contacted senior executives with ransom demands, which often took the form of emails like the one below[300]:

[297] Pierluigi Paganini, *HOW FAR DO STOLEN DATA GET IN THE DEEP WEB AFTER A BREACH?*, Security Affairs (Apr. 12, 2015), https://securityaffairs.com/35902/cyber-crime/propagation-data-deep-web.html.

[298] *Id.*

[299] Stefanie Schappert, Cl0p names first batch of alleged MOVEit victims, cybernews (June 15, 2023), https://cybernews.com/news/cl0p-moveit-ransom-attack-victims-names/; #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability, CISA (July 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[300] *#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, CISA (July 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

Figure 7

Figure 1: CL0P Ransom Note

Hello, this is the CL0P hacker group. As you may know, we recently carried out a hack, which was reported in the news on site [redacted].

We want to inform you that we have stolen important information from your GoAnywhere MFT resource and have attached a full list of files as evidence.

We deliberately did not disclose your organization and wanted to negotiate with you and your leadership first. If you ignore us, we will sell your information on the black market and publish it on our blog, which receives 30-50 thousand unique visitors per day. You can read about us on [redacted] by searching for CLOP hacker group.

You can contact us using the following contact information:x

unlock@rsv-box[.]com

and

unlock@support-mult[.]com

1191. CL0P also posted warnings on its own leak site, such as the one below[301]:

Figure 8

[301] Stefanie Schappert, *Cl0p names first batch of alleged MOVEit victims*, cybernews (June 15, 2023, 3:08 PM), https://cybernews.com/news/cl0p-moveit-ransom-attack-victims-names/.

1192. CL0P's first batch of targets, which included companies like Shell Global, were given until June 14, 2023, to provide ransom payments, or risk having their data exposed on the dark web.[302]

Figure 9

Ramson demand instructions posted on the Cl0p dark leak site

1193. In June of 2023, not even a month after the Data Breach was publicized, CL0P posted the first batch of organizations it claimed to have hacked by exploiting the MOVEit vulnerabilities. The victim list, which was posted to CL0P's dark web leak site, included U.S.-based financial services organizations 1st Source and First National Bankers Bank; Boston-based investment management firm Putnam Investments; the Netherlands-based Landal Greenparks; and the U.K.-based energy giant Shell.[303]

[302] *Id.*

[303] Carly Page, *Ransomware gang lists first victims of MOVEit mass-hacks, including US banks and universities*, TechCrunch (June 15, 2023, 2:34 AM), https://techcrunch.com/2023/06/15/moveit-clop-mass-hacks-banks-universities.

1194. The number of affected organizations has grown exponentially, with over 2,600 different entities within the United States alone.[304]

1195. Experienced cybersecurity professionals have acknowledged that the worst may not yet be over: the "broad scope of impact of the MOVEit vulnerability" ensures that more victims will have their Private Information exposed on both the dark and clear web, and that no one has a very good idea of when there might be a "light at the end of the tunnel."[305]

1196. Following the Data Breach, the Federal Bureau of Investigation and the Cybersecurity & Infrastructure Security Agency issued bulletins regarding the MOVEit vulnerabilities and CL0P's efforts to ransom the Private Information of Plaintiffs and Class Members.[306]

1197. The FBI and CISA have assembled a comprehensive breakdown of CL0P's exploitation of the MOVEit SQL injection zero-day vulnerability, which CL0P used to install a web shell named LEMURLOOT on MOVEit Transfer web applications, along with other malware.[307]

1198. The FBI and CISA also provided recommended mitigation strategies, some of which would have assisted in preventing CL0P from breaking into Defendants' systems.[308]

---

[304] Bert Kondruss, *MOVEit hack victim list*, Kon Briefing, https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html (last updated Dec. 20, 2023).

[305] Stefanie Schappert, *Cl0p names first batch of alleged MOVEit victims*, cybernews (June 15, 2023), https://cybernews.com/news/cl0p-moveit-ransom-attack-victims-names/.

[306] *Id.*

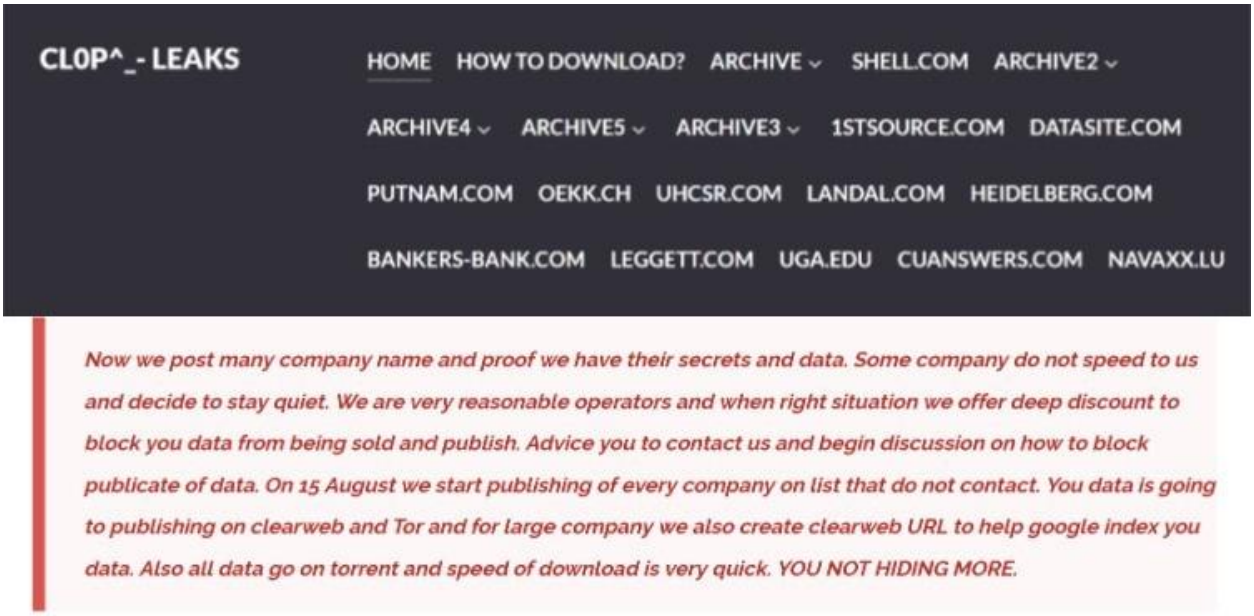
[307] *Id.*

[308] *Id.*

D. CL0P posted stolen data on the clear and dark web.

1199. While some companies that fell victim to the Data Breach immediately notified their constituencies, others kept mum, preferring to fly below the radar while negotiating with the hackers. This continued until August 15, 2023, when CL0P published all of the information it had stolen from hundreds of Data Breach targets who refused to pay.[309]

Figure 10



1200. After apparent negotiation breakdowns, Pricewaterhouse Coopers (PWC) became the first victim to get its own personalized clear web link, at which CL0P posted Torrent links for all the victim organizations it stole large caches from.[310]

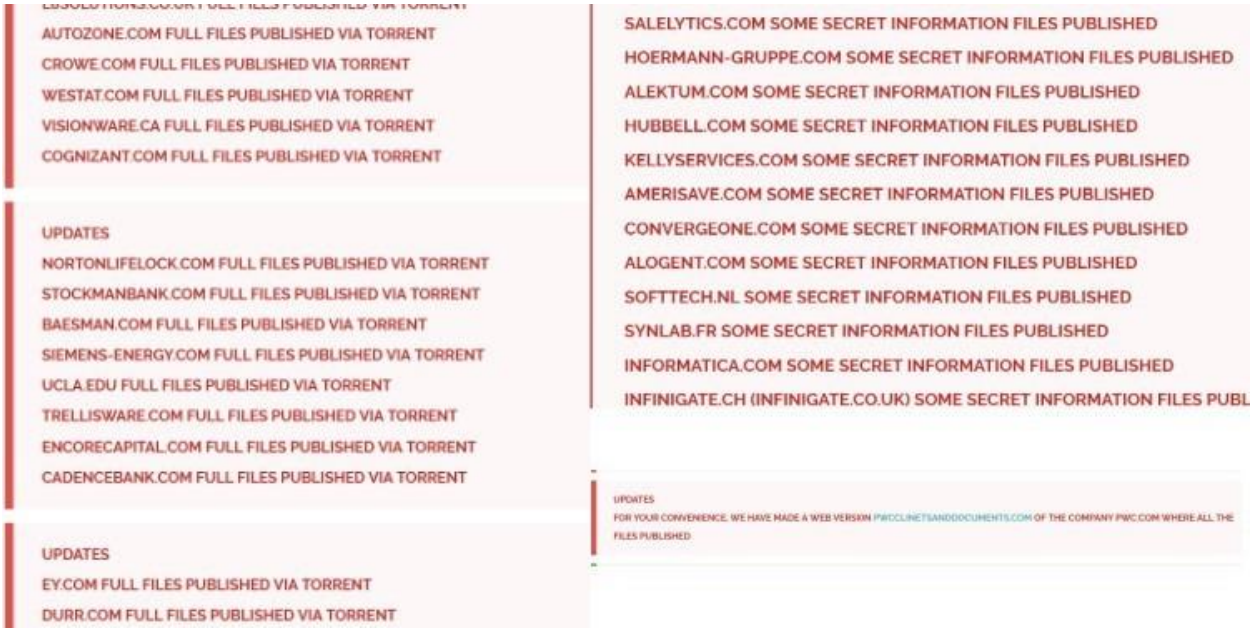
[309] Stefanie Schappert, *Cl0p names first batch of alleged MOVEit victims*, cybernews (June 15, 2023), https://cybernews.com/news/cl0p-moveit-ransom-attack-victims-names/.

[310] *Id.*

1201. Soon after, CL0P created websites for Aon, EY (Ernst & Young), Kirkland, and TD Ameritrade.[311]

1202. Since then, hundreds of caches of Private Information stolen from Defendants named in this action were posted on the clear web for open access.[312]

Figure 11



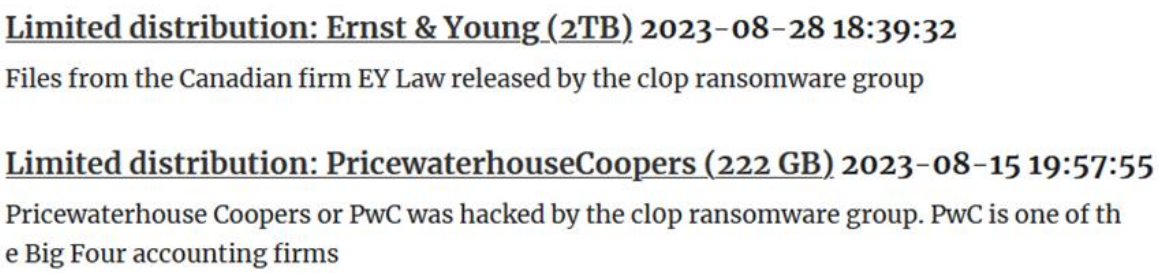
1203. For example, the dark web site Distributed Denial of Secrets has data from EY and PWC[313]:

---

[311] Lawrence Abrams, *Cl0p now leaks data stolen in MOVEit attacks on clearweb sites*, Bleeping Computer (July 23, 2023, 3:10 PM), https://www.bleepingcomputer.com/news/security/clop-now-leaks-data-stolen-in-moveit-attacks-on-clearweb-sites/.

[312] *Id.*; Stefanie Scappert, *Cl0p dumps all MOVEit victim data on Clearnet, threat insiders talk ransom strategy*, cybernews (Nov. 15, 2023, 12:53 PM), https://cybernews.com/security/clop-publish-all-moveit-victim-ransom-data-clearweb/; Lawrence Abrams, *Cl0p now leaks data stolen in MOVEit attacks on clearweb sites*, Bleeping Computer (July 23, 2023, 3:10 PM), https://www.bleepingcomputer.com/news/security/clop-now-leaks-data-stolen-in-moveit-attacks-on-clearweb-sites/.

[313] http://ddosxlvzzow7scc7egy75gpke54hgbg2frahxzaw6qq5osnzm7wistid.onion/wiki/Distributed_Denial_of_Secrets.



1204. Data stolen from PBI's MOVEit transfer server, which further contains data from dozens of PBI's clients, has been found and verified on the dark web.

1205. On November 11, 2024, a person or group known as Nam3L3ss was found to have posted 25 datasets containing millions of records of stolen employee data on the dark web. The data was compromised from MOVEit Transfer users and contained data from Amazon, MetLife, Cardinal Health, HSBC, Fidelity, US Bank, HP, Canada Post, Delta Airlines, Applied Materials, Leidos, Charles Schwab, 3M, Lenovo, Bristol Myers Squibb, Omnicom Group, TIAA, Union Bank of Switzerland, Westinghouse, Urban Outfitters, Rush University, British Telecom, Firmenich, City National Bank, and McDonald's. Nam3L3ss has stated that they possess many times more additional data that has not yet been released.[314]

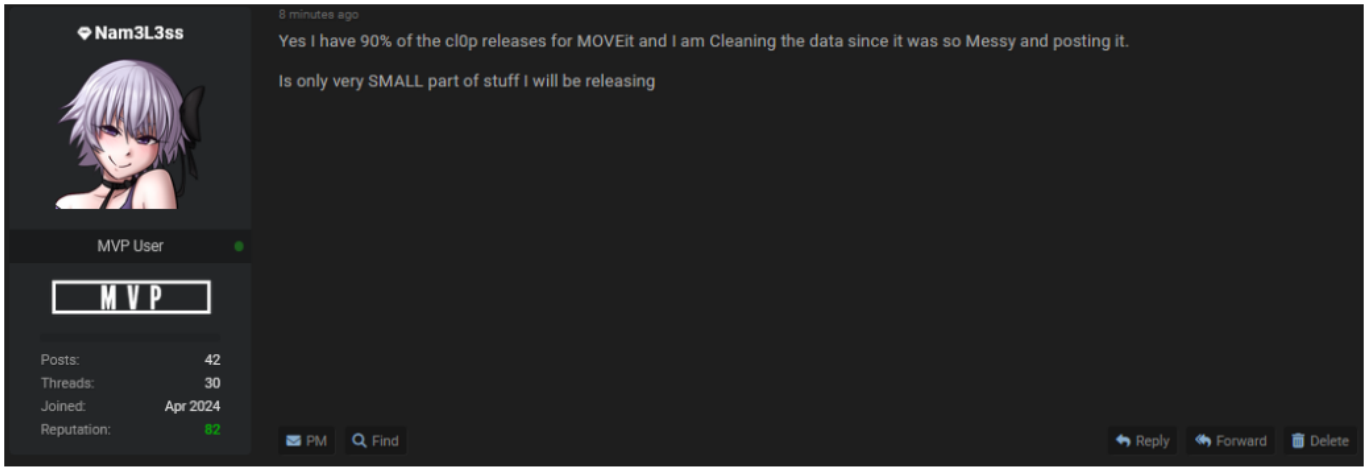
1206. Nam3L3ss obtained the stolen data from ransomware leak sites on the dark web after CL0P published torrents of the stolen data. It downloaded databases from ransomware websites and then converted the files to manageable .CSV database formats. From there, Nam3L3ss then "cleaned" the data, removing duplicates, irrelevant fields, and any data "that lacks

[314] Ernestas Naprys, *MOVEit fallout: hackers leak employee data from Amazon, MetLife, HSBC, and other major companies*, cybernews (Nov. 11, 2024, 4:09 PM), https://cybernews.com/security/moveit-fallout-hackers-leak-employee-data-from-amazon-metlife/; Sergiu Gatlan, *Amazon confirms employee data breach after vendor hack*, Bleeping Computer (Nov. 11, 2024, 2:10 PM), https://www.bleepingcomputer.com/news/security/amazon-confirms-employee-data-breach-after-vendor-hack/.

utility for cybercrime."[315] While information initially exposed from the MOVEit breach may have been difficult to categorize, Nam3L3ss has demonstrated that, not only is it able to organize the data, but it can also disclose only that data which hit has identified as most harmful to the victims—individual consumers—of the breach.

1207. Nam3L3ss claims to have 90% of the CL0P releases from the MOVEit breach, and intends to publish more information as it continues to "clean" the data, as outlined above.

Figure 12[316]



1208. Nam3L3ss's threats are not idle; since publishing information in November, it has continued to publish information exposed by the Data Breach, including information from Bank

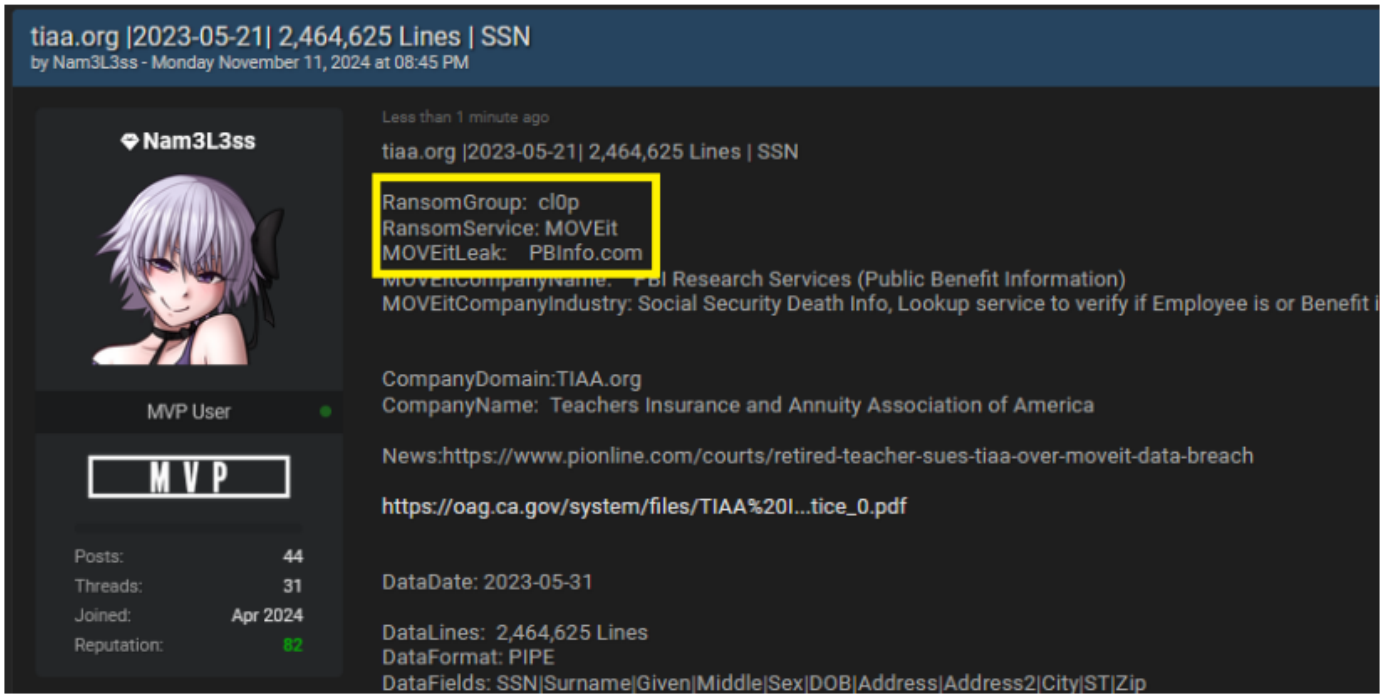
[315] *Inside the MOVEit Breach: How Cl0p and Nam3L3ss Expose Organizations to Ongoing Cyber Threats*, Foresiet (Nov. 12, 2024), https://foresiet.com/blog/inside-the-moveit-breach-how-cl0p-and-nam3l3ss-expose-organizations-to-ongoing-cyber-threats.

[316] *Id.*

of America, Koch, Nokia, JLL, Xerox, Morgan Stanley, and Bridgewater.[317] Researchers have confirmed the authenticity of the data.[318]

1209. Nam3L3ss's continued exposure of the MOVEit data includes information from PBI Bellwether Defendant TIAA, including Social Security numbers, names, addresses, sex, and date of birth.

Figure 13[319]



[317] Ionut Arghire, *760,000 Employee Records from Several Major Firms Leaked Online*, SecurityWeek (Dec. 3, 2024), https://www.securityweek.com/760000-employee-records-from-several-major-firms-leaked-online/.

[318] Sead Fadilpašić, *MOVEit breach chaos continues, data on hundreds of thousands leaked from Nokia, Morgan Stanley*, TechRadar (Dec. 3, 2024), https://www.msn.com/en-us/money/other/moveit-breach-chaos-continues-data-on-hundreds-of-thousands-leaked-from-nokia-morgan-stanley/.

[319] *Inside the MOVEit Breach: How Cl0p and Nam3L3ss Expose Organizations to Ongoing Cyber Threats*, Foresiet (Nov. 12, 2024), https://foresiet.com/blog/inside-the-moveit-breach-how-cl0p-and-nam3l3ss-expose-organizations-to-ongoing-cyber-threats.

1210. Nam3L3ss is intent on sharing all of the stolen data so that it is freely accessible to cybercriminals everywhere.[320] It is highly likely that, if information from a Defendant has not yet been exposed, it will be as Nam3L3ss continues to publish information.

1211. Accordingly, Plaintiffs and individual victims of the Breach will continue to be victimized as information obtained from the Breach will continue to proliferate on the dark web.[321]

E. CL0P's data destruction promises, like the promises of other cybercriminals, cannot be trusted.

1212. The United States government and other law enforcement agencies almost always advise against paying a ransom demand, and that is because cybercriminals cannot be trusted to do what they promise they will do in exchange for a ransom.

1213. Indeed, CL0P is infamous worldwide for their "signature double extortion strategy," which involves the encryption of files on the target's servers, followed by threats to publish the data on the dark or clear web for further exploitation or sale.[322]

1214. These tactics are explicitly exploitative: they hinge on extracting monetary concessions from targets based on the dual desires to regain access to their stolen information and contain the impact of the data breach (and potential liability incurred therefrom).

1215. Even in cases where Defendants paid a ransom to CL0P in exchange for decryption and/or promises not to post the stolen data on the clear web, there is no guarantee that the

---

[320] Alex Scroxton, *More data stolen in 2023 MOVEit attacks comes to light*, ComputerWeekly.com (Nov. 12, 2024, 4:10 PM), https://www.computerweekly.com/news/366615522/More-data-stolen-in-2023-MOVEit-attacks-comes-to-light.

[321] *Id.* ("Kevin Robertson, chief operating officer at Acumen Cyber, said: "This leak shows how data makes its way across the dark web, often reappearing in the news long after breaches took place and often in the hands of other attackers.").

[322] Stefanie Schappert, *Cl0p dumps all MOVEit victim data on Clearnet, threat insiders talk ransom strategy*, Cybernews (Nov. 15, 2023), https://cybernews.com/security/clop-publish-all-moveit-victim-ransom-data-clearweb/.

cybercriminals would honor their promises: the hackers could easily have re-copied the stolen data.[323]

1216. Indeed, data breach targets that pay ransom demands often cannot substantiate any claimed destruction or return of the data in question.[324]

1217. The FBI recognizes the likelihood that cybercriminals will renege on their promises once a ransom is paid, explaining that it "does not advocate paying a ransom, in part because it does not guarantee an organization will regain access to its data."[325]

1218. Several media outlets and industry groups have likewise questioned reliance on promises made by cybercriminals.[326]

1219. Indeed, many of the Defendants' data breach notifications advised affected individuals to monitor their own credit and financial accounts for suspicious activity.

---

[323] Gary Guthrie, *Paying to delete stolen data doesn't always work out for the victim, new study suggests*, ConsumerAffairs (Nov. 5, 2020), https://www.consumeraffairs.com/news/paying-to-delete-stolen-data-doesnt-always-work-out-for-the-victim-new-study-suggests-110520.html [https://perma.cc/DMV2-JRFP].

[324] *See* Leo Kelion & Joe Tidy, *National Trust joins victims of Blackbaud hack*, BBC News (July 30, 2020), https://www.bbc.com/news/technology-53567699 ("Although Blackbaud has said the cyber-criminals had provided confirmation that the stolen data was destroyed, one expert questioned whether such an assurance could be trusted. 'The hackers would know these people have a propensity to support good causes,' commented Pat Walshe from the consultancy Privacy Matters. This would be valuable information to fraudsters, he added, who could use it to fool victims into thinking they were making further donations when in fact they would be giving away their payment card details.") [https://perma.cc/NC7W-T9LJ]; *Phishing Scams Following Blackbaud Security Breach*, Mich. Dep't Att'y Gen., https://www.michigan.gov/ag/0,4534,7-359-81903_20942-540014--,00.html [https://perma.cc/E6K9-HVZZ].

[325] *High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations*, FBI (Oct. 2, 2019), https://www.ic3.gov/Media/Y2019/PSA191002 [https://perma.cc/VX8P-TW7F].

[326] *See, e.g.*, Phil Muncaster, *US Data Breach Volumes Plummet 30% in 2020*, Infosecurity Mag. (Oct. 15, 2020), https://www.infosecurity-magazine.com/news/us-data-breach-volumes-plummet-30/ [https://perma.cc/2LYC-XDP6]; Zack Whittaker, *Decrypted: The Major Ransomware Attack You Probably Didn't Hear About*, TechCrunch (Oct. 7, 2020), https://techcrunch.com/2020/10/07/decrypted-blackbaud-ransomware-attack-gets-worse/ [https://perma.cc/R8M4-FMMC].

F. Individual victims of cybercriminal data breaches face immediate and significant harm.

1220. Private Information is valuable property. Its value is axiomatic, considering the market value and profitability of "Big Data" to corporations in America. Illustratively, Alphabet Inc., the parent company of Google, reported in its 2020 Annual Report a total annual revenue of $182.5 billion and net income of $40.2 billion.[327] $160.7 billion of this revenue derived from its Google business, which is driven almost exclusively by leveraging the Private Information it collects about users of its various free products and services.

1221. Criminal law also recognizes the value of Private Information and the serious nature of the theft of Private Information by imposing prison sentences. This strong deterrence is necessary because cybercriminals extract substantial revenue through the theft and sale of Private Information. Once a cybercriminal has unlawfully acquired Private Information, the criminal can demand a ransom or blackmail payment for its destruction, use the Private Information to commit fraud or identity theft, or sell the Private Information to other cybercriminals on the black market.

1222. Cybercriminals use "ransomware" to make money and harm victims. Ransomware is a widely-known and foreseeable malware threat in which a cybercriminal encrypts a victim's computer such that the computer's owner can no longer access any files or use the computer in any way. The cybercriminal then demands a payment for the decryption key. Ransomware is typically propagated through phishing, spear phishing, or visiting a malicious or compromised website that contains a virus or other malware.

1223. Once stolen, Private Information can be used in many ways. Private Information can be offered for sale on the dark web, a heavily encrypted part of the Internet that makes it

[327] Alphabet Inc., Annual Report (Form 10-K) at 32 (Feb. 3, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm.

difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and Private Information. Websites appear and disappear quickly, making it a dynamic environment.

1224. The U.S. Government Accountability Office ("GAO") released a report in 2007 regarding data breaches, finding that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[328]

1225. The GAO Report explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name." The GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[329]

1226. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[330] According to Experian, "[t]he

[328] Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown ("GAO Report") at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf [https://perma.cc/GCA5-WYA5].

[329] *Id*.

[330] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things: "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to, among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; or use the victim's information in the event of arrest or court action.[331]

1227. With access to an individual's Private Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and Social Security number to obtain government benefits; filing a fraudulent tax return using the victim's information; or committing healthcare fraud using information related to an individual's health insurance. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[332]

1228. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[333]

1229. Theft of Social Security numbers creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new Social Security

---

[331] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Private Information and How Can You Protect Yourself*, Experian (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/

[332] *Id.*

[333] *Id.*

number, a breach victim has to demonstrate ongoing harm from misuse of their Social Security number, and a new Social Security number will not be provided until after the harm has already been suffered by the victim.

1230. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (*e.g.*, name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating: "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[334]

1231. Beyond monetary losses and healthcare fraud, data breaches also have a deep, psychological impact on their victims.

> In some ways, a cyber attack can feel like the digital equivalent of getting robbed, with a corresponding wave of anxiety and dread. Anxiety, panic, fear, and frustration—even intense anger—are common emotional responses when experiencing a cyber attack. While expected, these emotions can paralyze you and prolong or worsen a cyber attack.[335]

G. It is reasonable for individual victims of cybercriminal data breaches to take actions to mitigate their risk of harm.

1232. Cybercriminals can and do use the Private Information that Defendants were entrusted to safeguard to perpetrate financial crimes that harm Plaintiffs and the Class Members.

1233. In addition to all the other immediate consequences of the Data Breach, Plaintiffs and Class Members face a substantially increased risk of identity theft and fraud.

---

[334] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, Time (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[335] Amber Steel, *The Psychological Impact of Cyber Attacks*, LastPass (Aug. 17, 2022), https://blog.lastpass.com/posts/the-psychological-impact-of-cyber-attacks.

1234. The Federal Trade Commission ("FTC") recommends that identity theft victims take several steps to protect their Private Information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[336]

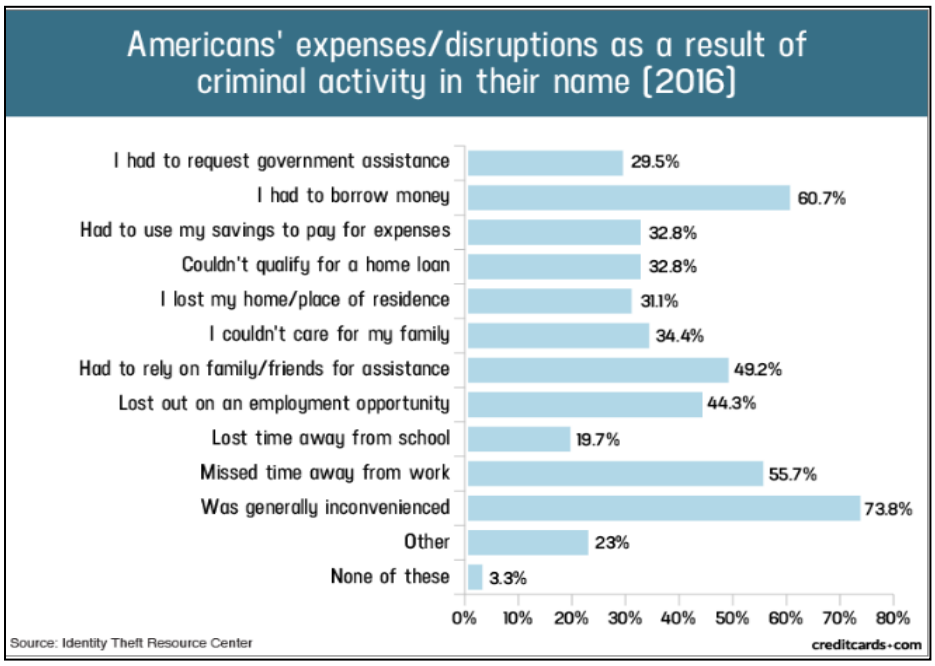
1235. Cybercriminals use stolen PII such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

1236. A study by the Identity Theft Resource Center ("ITRC") shows the multitude of harms caused by fraudulent use of personal and financial information[337]:

[336] Identity Theft Recovery Steps, FTC, https://www.identitytheft.gov/Steps (last visited Nov. 26, 2024). Indeed, the FTC takes data breaches seriously, and has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information can constitute an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[337] Jason Steele, Credit Card and ID Theft Statistics, Creditcards.com (June 11, 2021), https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/.

Figure 14



1237. As set forth above, 96.7% of study subjects experienced costs or other harms from the criminal activity.[338] As illustrated in the above graphic, this includes devastating results such as: "I lost my home/place of residence" and "I couldn't care for my family." Moreover, the harms of identity theft are not limited to the affected individual and may adversely impact other associated persons and support systems, including government assistance programs. In the ITRC study, nearly one-third of survey respondents had to request government assistance because of identity theft, such as welfare, EBT, food stamps, or similar support systems.[339] The ITRC study concludes that "identity theft victimization has an extreme and adverse effect on each individual as well as all of the support systems and people associated with the individual."[340]

[338] *Id.*

[339] *Id.*

[340] *Id.*

1238. Private Information is a valuable property right.[341] Its value is axiomatic, considering the value of Big Data in corporate America as well as the consequences of cyber thefts resulting in heavy prison sentences. This obvious risk to reward analysis illustrates that Private Information has considerable market value that is diminished when it is compromised.

1239. There may also be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the GAO Report: "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[342]

1240. Private Information is such an inherently valuable commodity to identity thieves that, once it is compromised, criminals often trade the information on the cyber black-market for years.

1241. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[343]

---

[341] *See, e.g.*, John T. Soma, et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 1, 2 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.").

[342] Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown ("GAO Report") at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf [https://perma.cc/GCA5-WYA5].

[343] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 PM), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

1242. Medical identity theft "is also more difficult to detect, taking almost twice as long as normal identity theft."[344] In warning consumers of the dangers of medical identity theft, the FTC states that an identity thief may use Private Information "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[345] The FTC also warns, "If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[346]

1243. A report published by the World Privacy Forum[347] and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

a. Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

b. Significant bills for medical goods and services not sought or received.

c. Issues with insurance, co-pays, and insurance caps.

d. Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

e. Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due

[344] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, World Privacy Forum (Dec. 12, 2017), https://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

[345] *See* FBI, Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain (Apr. 8, 2014) at 14, https://publicintelligence.net/fbi-health-care-cyber-intrusions/.

[346] *See What to Know About Medical Identity Theft*, FTC, https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Nov. 26, 2024).

[347] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, World Privacy Forum (Dec. 12, 2017), https://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

f. As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgages or other loans and may experience other financial impacts.

g. Phantom medical debt collection based on medical billing or other identity information.

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.

1244. Furthermore, data breaches that expose any personal data, and in particular non-public data of any kind (*e.g.*, donation history or hospital records), directly and materially increase the chance that a potential victim is targeted by a spear phishing attack in the future, and spear phishing results in a high rate of identity theft, fraud, and extortion.[348]

1245. The United States Court of Appeals for the First Circuit has recognized that it is not necessary for a victim of a data breach to have their identity stolen, or to suffer actual fraud, for it to be reasonable for a data breach victim to take steps to protect themselves.[349]

[348] *See* Leo Kelion & Joe Tidy, *National Trust joins victims of Blackbaud hack*, BBC News (July 30, 2020), https://www.bbc.com/news/technology-53567699 (concluding that personal information such as "names, titles, telephone numbers, email addresses, mailing addresses, dates of birth, and, more importantly, donor information such as donation dates, donation amounts, giving capacity, philanthropic interests, and other donor profile information . . . . in the hands of fraudsters, [makes consumers] particularly susceptible to spear phishing—a fraudulent email to specific targets while purporting to be a trusted sender, with the aim of convincing victims to hand over information or money or infecting devices with malware").

[349] *Webb v. Injured Workers Pharmacy, LLC*, 72 F.4th 365, 371 (1st Cir. 2023). In *Webb*, the First Circuit concluded that "plausible allegations of actual misuse [of PII] . . . state a concrete injury under Article III." *Webb*, 72 F.4th at 373. The First Circuit is in agreement with other circuits that have encountered the same question. *See, e.g.*, *In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1262 (11th Cir. 2021); *Attias v. CareFirst, Inc.*, 865 F.3d 620, 627 (D.C. Cir. 2017); *In re Marriott, Int'l, Inc. Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 459 (D. Md. 2020); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 690 (7th Cir. 2015) ("customers should not have to wait until hackers commit identity theft or credit-card fraud" in order for their mitigation efforts to be reasonable and compensable).

1246. As the United States Court of Appeals for the Seventh Circuit aptly observed almost a decade ago: "the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."[350]

1247. This remains true, ten years later. The intent of hackers (such as CL0P) is clear when they hack systems, such as the Defendants': they are attempting to access consumers' Private Information for the purpose of ransoming it back, and/or selling it for a profit.

1248. There may be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average, it takes approximately three months for a consumer to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[351]

1249. In addition, there is a strong probability that much of the information stolen in the Data Breach has not yet been made available on the black market in a coherent, organized fashion,[352] meaning Plaintiffs and Class Members will remain at an increased risk of fraud and identity theft for many years into the future. Indeed, some Class Members are in very early stages of their lives—in their twenties and thirties. Thus, as the respective Data Breach Notices advise, customers, including Plaintiffs and Class Members, must vigilantly monitor their financial accounts for many years to come.

---

[350] *Remijas*, 794 F.3d at 693.

[351] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

[352] Stefanie Schappert, *Cl0p names first batch of alleged MOVEit victims*, cybernews (June 15, 2023, 3:08 PM), https://cybernews.com/news/cl0p-moveit-ransom-attack-victims-names/; (describing certain data stolen from MOVEit customers and put on the clear web by Cl0p as "a challenge for us to download," and noting that the data is "unstructured.").

H. Defendants' actions have been insufficient to protect consumers or compensate victims.

1250. The Defendants in this action did not take sufficient steps to protect their customers (and/or their customers' customers), and have not done nearly enough to compensate the victims of the Data Breach, who will suffer real harm for years to come.

1251. As an initial matter, Defendants did not take the most basic steps to ensure network security.

1252. The industries that Defendants serve have seen a substantial increase in cyberattacks and data breaches since as early as 2016.[353]

1253. Indeed, cyberattacks have become so notorious that the FBI and Secret Service issued a warning in 2019 to potential targets so they were aware of, and prepared for, a potential attack.[354]

1254. Cybersecurity efforts have developed apace to provide an answer to these rising attacks and multiplying attack vectors. In 2019, both Microsoft and Google publicly reported that using multi-factor authentication ("MFA") blocks more than 99% of automated hacks, including most ransomware attacks that occur because of unauthorized account access. Likewise, the reputable SANS Software Security Institute issued a paper stating: "[t]ime to implement multi-factor authentication!"[355] An example of MFA implementation is receiving a text with a code when you input your username and password into a website; even if a cybercriminal knew your username

[353] *Id.*

[354] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware [https://perma.cc/Z6GF-777F].

[355] Matt Bromiley, *Bye Bye Passwords: New Ways to Authenticate*, SANS Software Security Inst. (July 2019), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ.

and password, the cybercriminal would not be able to see the code on your phone and would thus be blocked from accessing your online account.

1255. In this regard, implementing MFA "can block over 99.9 percent of account compromise attacks."[356]

1256. The FBI concurs, listing "applying two-factor authentication wherever possible" as a best practice to defend against ransomware attacks.[357]

1257. Cybersecurity experts agree: "MOVEit should be behind technologies that provide access to only those who need it via tools such as Zero Trust (*e.g.*, access gateways secured by MFA) or simple allowlists and blocklists."[358]

1258. Experts further recommend: "If you run MOVEit within your organization, ensure that the database runs as a specific user that can only interact with MOVEit and not as a superuser with broader access. The exploit utilizes SQL injection to allow attackers to manipulate server databases and execute arbitrary code, resulting in data exfiltration. Because this breach is an SQL injection leading to remote code execution (RCE), the adversary only gains initial access to the database server and user."[359]

1259. Defendants also could have employed (either internally or through third parties) competent professionals to act as 24/7 "eyes on glass." Providers of managed security services,

---

[356] *What Is Multi-Factor Authentication (MFA)?*, Consensus Technologies (Sept. 16, 2020), https://www.concensus.com/blog/what-is-multi-factor-authentication/.

[357] Ransomware Victims Urged to Report Infections to Federal Law Enforcement, FBI (Sept. 15, 2016), https://www.ic3.gov/PSA/2016/psa160915.

[358] *Three Steps to Prevent a Cybersecurity Breach from MOVEit Exploit*, SecurityScorecard (June 7, 2023), https://securityscorecard.com/blog/three-steps-to-prevent-a-cybersecurity-breach-from-moveit-exploit-securityscorecards-investigation-into-zellis-reach-uncovers-2500-exposed-moveit-servers-across-790-organizations/.

[359] *Id.*

also referred to as "managed detection and response" ("MDR") employ a sophisticated series of artificial and human intelligence to monitor for signs that a breach is underway.

1260. The MOVEit SQL injection vulnerability was exploited by CL0P in order to execute a series of commands that ultimately resulted in the exfiltration of data. Either on their own or through the use of a qualified third-party vendor, Defendants could and should have been monitoring their own systems and repositories for indications of compromise ("IOCs,"), which would have included external injection of SQL code by unauthorized users. Companies have an obligation to monitor their systems for the execution of unauthorized code. If Defendants had appropriate monitoring in place, they could have detected, and prevented this attack.

1261. Indeed, companies who were using appropriate managed security detected the MOVEit vulnerability as early as May 27, 2023, and were able to take steps to prevent the large-scale exfiltration of consumers' sensitive information. For instance, on May 27, 2023, researchers for Akamai (a cybersecurity company) fended off an attempt by CL0P to use the MOVEit exploitation against one of Akamai's financial customers, "an attack that was blocked by the Akamai Adaptive Security Engine."[360]

1262. There were services available for Defendants to detect the Data Breach and prevent large scale exfiltration of the Private Information entrusted to them, but Defendants simply failed to appropriately implement these services.

1263. Furthermore, it does not take cybersecurity expertise to know Defendants should not have maintained—or allowed the maintenance of—millions of consumers' Private Information on MOVEit software, where it was a sitting duck waiting for a cyberattack such as the Data Breach.

[360] Akamai Security Intelligence Group, *MOVEit SQLi Zero-Day (CVE-2023-34362) Exploited by CL0P Ransomware Group*, Akamai (June 8, 2023), https://www.akamai.com/blog/security-research/moveit-sqli-zero-day-exploit-clop-ransomware.

1264. There were plenty of technologies and processes readily available that Defendants could have utilized to prevent the Data Breach. Defendants failed to do so.

1265. The problem caused by Defendants' unwillingness to take proper data security precautions will only get worse: a study published in May 2022 by the International Data Corporation projects that the amount of new data created, captured, replicated, and consumed is expected to double in size by 2026.[361]

1266. With an increase in data creation comes a heightened risk of data breaches and bad actors gaining access to personal information. One result of data breaches, identity theft, poses a serious threat to consumers engaging in online transactions and across a host of digital platforms. Both state and federal laws and regulations impose standards of reasonable security measures for businesses so consumers can, in turn, feel safe sharing their Private Information in the marketplace.

1267. Data privacy is important to the public: according to a survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[362]

1268. Data breaches are not an unpreventable occurrence. In the Data Breach and Encryption Handbook, Lucy Thompson wrote, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of

[361] *See* John Rydning, *Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth*, IDC (Nov. 2022), https://www.linkedin.com/embeds/publishingEmbed.html?articleId=7080078918768595657.

[362] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 11, 2016), https://library.cyentia.com/report/report_001510.html .

appropriate security solutions." She continued, "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[363]

1269. The Defendants in these consolidated cases knew there were steps they could take to secure their systems and protect the Private Information of their customers; they simply chose not to take them.

I. Damages can compensate victims for the harm caused by the breach.

1270. To the injury of failing to protect their systems with readily available technology services designed to curtail or prevent data breaches like the Data Breach, resulting in the exposure of Plaintiffs' and Class Members' Private Information, Defendants have added the insult of refusing to provide even paltry compensation.

1271. While several Defendants have offered victims of the Data Breach credit monitoring services, these services alone are not enough: a year or two of credit monitoring will not un-ring the bell of the release of the Private Information of the Plaintiffs and Class Members, which will circulate through the various levels of the internet (clear, dark, and deep) for years and years, if not in perpetuity. Particularly considering the fact that Social Security numbers were exposed in the Data Breach, Data Breach victims will need to monitor their credit and accounts for years and years to come—and these services are typically accounted for in settlements and judgments involving data breaches.[364]

---

[363] Lucy L. Thomson, Data Breach and Encryption Handbook (Am. Bar Assoc. 2011).

[364] For instance, in July 2019, the CFPB, FTC and States announced a settlement with Equifax over the 2017 Equifax data breach, which included up to ten years of credit monitoring and identity restoration services. *See CFPB, FTC and States Announce Settlement with Equifax Over 2017 Data Breach,* CFPB (July 22, 2019), https://www.consumerfinance.gov/about-us/newsroom/cfpb-ftc-states-announce-settlement-with-equifax-over-2017-data-breach/.

1272. The Private Information exposed in the Data Breach has real value, as explained above. Plaintiffs and the Class Members have therefore been deprived of their rights to the control of that property and have lost the value they might otherwise have incurred from that data.[365]

1273. Plaintiffs and the Class Members have spent significant time, and will spend more, monitoring their accounts, changing login credentials, and recovering from the inevitable fraud and identity theft which will occur, which deserves to be compensated: Defendants have not made apportionment for this very real injury.[366]

1274. Similarly, Defendants have offered no compensation for the aggravation, agitation, anxiety, and emotional distress that Plaintiffs and the Class Members have suffered, and will continue to suffer, as a result of the Data Breach: the knowledge that their information is out in the open, available for sale and exploitation at any time in the future is a real harm that also deserves compensation.

1275. Plaintiffs and Class Members were also deprived of the benefit of their bargain when they interacted with Defendants: each Defendant had a duty to take reasonable steps to protect the Private Information of its customers. This duty was inherent in the relationships between Plaintiffs and Class Members and Defendants, whether through express contractual terms, implied contractual terms, or statutory or implied duties of good faith and fair dealing.

1276. Defendants have not taken sufficient steps or even attempted to make their customers, the real victims in this Data Breach, whole. Defendants have failed their duty to protect

[365] Ravi Sen, *Here's how much your personal information is worth to cybercriminals – and what they do with it*, PBS (May 14, 2021, 12:04 PM), https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it.

[366] Time spent monitoring accounts is another common and cognizable, compensated harm in data breach cases. *See Equifax Data Breach Settlement*, FTC, https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement (last visited Nov. 26, 2024).

Plaintiffs' and Class Members' Private Information and have failed in their duty to help these consumers protect themselves in the future.

1277. Any monitoring or identity theft protection that Defendants have offered is insufficient, as individuals will be subjected to harm as a result of the breach for years to come. Significantly, information continues to be published by threat actors and cybercriminals online from the breach; identity theft protection and credit monitoring for a short period of time cannot sufficiently protect consumers, who need to be diligent for likely the rest of their lives. Additionally, identity theft and credit monitoring services are insufficient to protect consumers from certain scams, phishing attempts, malware, and additional extortion that they will likely face and have already faced as a result of the breach.

J. This case demonstrates that the risk of harm and class member injuries are not hypothetical.

1278. Plaintiffs who have filed suit in this multidistrict litigation have suffered injuries in a number of ways, including:

a. Loss of benefit of their bargain, for individuals who provided compensation to entities to safely transfer and store their data with one of the Defendants or Defendants' vendors;

b. Loss of value of their personal information, in that it has been misused for purposes to which they did not consent, and they have not been properly compensated for this misuse;

c. Actual or attempted fraud, misuse, or identity theft caused by the Data Breach, including, but not limited to, their information being published to the clear, deep, and dark web; as well as

d. Time and expenses that were reasonably spent to mitigate the impact of the breach.

1279. Several Plaintiffs have already experienced actual or attempted fraud, which is reasonably related to the Data Breach, which demonstrates that the Data Breach has put them at immediate risk for additional harm.

1280. The fraud and attempted fraud that certain Plaintiffs have suffered is sufficiently related to the Data Breach because of the time frame in which it occurred (after the Data Breach), and because the same information that was exposed in the Data Breach would have been used to effectuate the fraud and identity theft.

1281. The harm already suffered by Plaintiffs demonstrates that the risk of harm is ongoing.

K. Defendants Failed to Provide Adequate Identity Theft and Credit Monitoring Protection to Individuals Impacted by the Data Breach.

1282. "Credit monitoring" generally refers to services that will provide real-time alerts to a consumer regarding any changes in their credit report, e.g., when a new loan is opened in their name. These services allow the consumer to investigate any suspicious activity that might have resulted from the fraudulent use of their PII.

1283. Through credit monitoring, consumers get alerts very fast, thus creating the capability for timely action against possible identity theft or other crimes. These alerts reduce damages and potentially increase the possibility to fix problems before they become unmanageable.

1284. "Identity protection" services or products, on the other hand, refer to monitoring and related services that track and protect much more than consumers' credit. Identity monitoring services, for example, monitor a consumer's PII—across public records, the dark web, etc.—and alert the consumer if anything suspicious occurs.

1285. Yet, the reality is that if an identity service detects that something suspicious has happened with a consumer's PII, it is likely already too late to fully prevent cyber bad attacks from abusing that consumer's information. For this reason, effective identity protection services also

include robust support—including identity theft insurance—for consumers who have already been the victim of identity theft, helping them to mitigate the consequences of such theft.

1286. The free services offered by Defendants are insufficient to protect Plaintiffs from further identity theft and fraud, both in duration (most commonly only 12-24 months) and services. Indeed, cyber bad actors are fully aware that credit monitoring and identity protection services offered by corporations are temporary. Such is the case here, where Defendants offered individuals impacted by its Data Breach as little as 12-24 months of free credit and/or identity monitoring services.

1287. A growing number of companies now offer free credit monitoring and identity protection services after a data breach. But a year-long—or even a lifetime—offer of such services only benefits consumers impacted by a data breach if the specific services provided are comprehensive and effective.

1288. In other words, the fine print of a credit monitoring and identity protection product matters *significantly*. Defendants' provision of a limited, low-quality product for 12-24 months is of little value to Plaintiffs and Class Members and, in fact, may actually do a disservice by providing consumers with a false sense of security.

1289. In light of the PII that was compromised in the Data Breach, all individuals for whom such information was exposed require lifetime credit monitoring and identity protection services that include the following features:

a. *Real-Time Alerts*: Instant notifications of any suspicious activities, such as new credit inquiries, account openings, or changes to PII.

b. *Comprehensive Credit Report Access*: Access to credit reports from all three major credit bureaus (Equifax, Experian, and TransUnion) to ensure a complete overview of the PII victim's current credit status.

c. *Credit Lock and Freeze Services*: The ability to easily lock or freeze credit reports to prevent new accounts from being opened in the victim's name without their authorization.

d. *Regular Updates and Reports*: Periodic summaries of monitoring activities and any alerts or changes detected, helping users stay informed about their credit health.

e. *Credit Score Monitoring*: Regular updates and alerts regarding changes in credit scores, which can indicate potential identity theft or unauthorized activities.

f. *Dark Web Monitoring*: Continuous scanning of dark web sites and forums for stolen PII, such as Social Security numbers, credit card details, and other PII.

g. *Public Records Monitoring*: Alerts about any changes or new entries in public records, such as bankruptcies, liens, or court judgments.

h. *Financial Account Monitoring*: Surveillance of bank accounts, credit cards, and other financial accounts for suspicious transactions and unauthorized activities.

i. *Social Security Number Monitoring*: Alerts if the Social Security number is used in ways that are inconsistent with the user's normal activities or geographic location.

j. *Data Breach Notifications*: Timely alerts about data breaches that could affect the user's PII, along with guidance on steps to take if affected.

k. *Child Identity Monitoring*: Monitoring services that protect children's identities, as children's Social Security numbers are often targeted by thieves.

l. *Medical Identity Monitoring*: Alerts for any activities related to medical insurance or healthcare services to prevent and detect medical identity theft.

m. *Fraud Resolution Assistance*: Dedicated support from specialists to help resolve issues arising from identity theft and guide victims through the recovery process.

n. *Educational Resources*: Access to resources and tools that educate users on how to protect their identity, recognize potential threats, and understand their credit reports.

o. *Identity Theft Insurance*: Coverage for expenses related to identity theft, including legal fees, lost wages, and other recovery costs.

III. Preventing the Data Breach.

1290. Progress could have prevented the Data Breach by following industry standards for secure software development and maintenance.[367]

1291. The remaining Defendants could also have prevented or mitigated against the risk of the Data Breach through implementation of security-standard data management, software review, data mapping, risk management, employment of zero-trust policies, and diligence concerning Progress's software.

A. Secure software development.

1292. Progress could have prevented the Data Breach by following secure software development practices by default, rather than seeking to maintain and patch outdated software with critical security vulnerabilities for decades.[368]

1293. Secure software development "focuses on identifying and mitigating security risks from the early stages of development to the deployment and maintenance phases."[369]

1294. Secure software development includes[370]:

a. Threat modeling

b. Secure coding practices

c. Secure code review and testing

d. Security training and awareness

e. Ongoing maintenance and updates

---

[367] *MOVEit Data Breach: Summary and How to Prevent SQL Injection Attacks*, TitanFile, https://www.titanfile.com/blog/moveit-data-breach-summary-and-how-to-prevent-sql-injection-attacks/ (last visited Nov. 26, 2024).

[368] *Id.*

[369] *Id.*

[370] *Id.*

1295. Following secure software development practices from the beginning of development through release and maintenance of the software is an industry standard and best practice because it avoids the potential for overlooking a security vulnerability in outdated code.[371]

1296. Secure software development is an industry standard, evidenced by the major industry organizations that adhere to and publish these standards:

a. Microsoft—which maintains the .NET framework on which MOVEit was developed—specifically instructs developers to review code for SQL injection vulnerabilities.[372] As early as 2008, Microsoft offered a free utility that would scan source code for possible SQL injection vulnerabilities.[373] Microsoft also provides guidance for vendors to check applications and websites for SQL injection.[374]

b. Oracle secure coding standards emphasize security throughout the development lifecycle, including in planning and design.[375]

---

[371] *Id.*

[372] *CA3001: Review code for SQL injection vulnerabilities*, Microsoft Learn Challenge (Apr. 22, 2023), https://learn.microsoft.com/en-us/dotnet/fundamentals/code-analysis/quality-rules/ca3001; *CA2100: Review SQL queries for security vulnerabilities*, Microsoft Learn Challenge (Sept. 13, 2024), https://learn.microsoft.com/en-us/dotnet/fundamentals/code-analysis/quality-rules/ca2100; *Security Considerations (Entity Framework)*, Microsoft Learn Challenge (Nov. 6, 2021), https://learn.microsoft.com/en-us/dotnet/framework/data/adonet/ef/security-considerations; *Writing secure dynamic SQL in SQL Server*, Microsoft Learn Challenge (Nov. 18, 2022), https://learn.microsoft.com/en-us/sql/connect/ado-net/sql/writing-secure-dynamic-sql?view=sql-server-ver16; *Configuring parameters and parameter data types*, Microsoft Learn Challenge (Sept. 15, 2021), https://learn.microsoft.com/en-us/dotnet/framework/data/adonet/configuring-parameters-and-parameter-data-types

[373] SQL-Server-Team, *Getting started with Microsoft ® Source Code Analyzer for SQL Injection*, SQL Server Blog (Mar. 23, 2019), https://techcommunity.microsoft.com/t5/sql-server-blog/getting-started-with-microsoft-174-source-code-analyzer-for-sql/ba-p/383452

[374] Paul Litwin, *Stop SQL Injection Attacks Before They Stop You*, Microsoft Learn Challenge (Oct. 11, 2019), https://learn.microsoft.com/en-us/archive/msdn-magazine/2004/september/data-security-stop-sql-injection-attacks-before-they-stop-you.

[375] *Coding Standards*, Oracle https://www.oracle.com/corporate/security-practices/assurance/development/ (last visited Nov. 26, 2024).

c. Apple's secure coding standards describe validating input, which would mitigate or prevent SQL injection.[376]

d. Carnegie Mellon Software Engineering Institute Secure Coding standards describe several techniques that would have prevented this Data Breach, including validate input, default deny, and least privilege.[377]

e. OWASP Secure Coding Practices specifically address preventing SQL Injection.[378]

f. NIST publishes a Secure Software Development Framework which focuses on avoiding the vulnerabilities that caused this Data Breach.[379]

1297. Progress and its predecessors failed to follow secure software development practices from the initial development of MOVEit Transfer because they included code with critical security vulnerabilities—including code susceptible to SQL injection—and then overlooked or did not attempt to discover such vulnerabilities when maintaining the software.[380]

B. Monitoring potential security risks.

1298. Progress could have prevented the Data Breach by monitoring potential security risks identified by the software development industry.[381]

---

[376] *Introduction to Secure Coding Guide*, (Apple) Developer, https://developer.apple.com/library/archive/documentation/Security/Conceptual/SecureCodingGuide/Introduction.html (last visited Nov. 26, 2024).

[377] Robert Seacord, *Top 10 Secure Coding Practices*, Carnegie Mellon U. Software Eng'g Inst., https://wiki.sei.cmu.edu/confluence/display/seccode/Top+10+Secure+Coding+Practices (last updated May 2, 2018).

[378] *Secure Coding Practices*, OWASP, https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/ (last visited Nov. 26, 2024).

[379] Secure Software Development Framework, NIST, https://csrc.nist.gov/projects/ssdf (last visited Nov. 26, 2024).

[380] *Id.*

[381] *Id.*

1299. The software development industry publishes numerous resources for developers to learn about old, new, and emerging areas of potential vulnerability, such as the OWASP Top 10, which lists the 10 most serious potential security vulnerabilities in the industry today.[382]

1300. SQL injection is the third most critical security risk on the OWASP Top 10.[383]

1301. SQL injection is frequently discussed as a widespread and easy to prevent vulnerability.[384]

1302. Vulnerable and outdated components are the sixth most critical security risk on the OWASP Top 10.[385]

1303. The BinaryFormatter.Deserialize remote code execution vulnerability has been documented and easy to prevent since at least 2017.[386]

1304. Monitoring developments in software security from industry resources is a best practice because it flags old, new, and emerging areas of potential vulnerability.[387]

1305. Progress failed to monitor potential security risks because they included code in MOVEit Transfer with critical security vulnerabilities—such as SQL injection and

---

[382] *Id.*

[383] OWASP Top Ten, *Top 10 Web Application Security Risks*, https://owasp.org/www-project-top-ten/ (last visited Nov. 26, 2024).

[384] Kinza Yasar et al., *Definition: SQL injection (SQLi)*, TechTarget (Apr. 2023), https://www.techtarget.com/searchsoftwarequality/definition/SQL-injection.

[385] OWASP Top Ten, *Top 10 Web Application Security Risks*, https://owasp.org/www-project-top-ten/ (last visited Nov. 26, 2024).

[386] BinaryFormatter serialization methods are obsolete and prohibited in ASP.NET apps, supra note 77; A8:2017-Insecure Deserialization, supra note 80; OWASP Top 10, supra note 64; pwntester, supra note 82.

[387] *MOVEit Data Breach: Summary and How to Prevent SQL Injection Attacks*, TitanFile, https://www.titanfile.com/blog/moveit-data-breach-summary-and-how-to-prevent-sql-injection-attacks/ (last visited Nov. 26, 2024).

deserialization—that are frequently identified by the software development industry as critical potential vulnerabilities.[388]

C. Sanitizing and validating user input.

1306. Progress could have prevented the Data Breach by designing MOVEit Transfer to sanitize and validate user input, rather than "trusting" user input as safe.[389]

1307. Sanitizing and validating user input is an industry standard and best practice because it ensures that data meets the criteria expected by the software, whether authorized or malicious, and stops potential sources of malicious code from reaching the database.[390]

1308. Progress failed to sanitize and validate user input because they allowed MOVEit Transfer to pass user input directly to the SQL engine, such that malicious code within user input could be executed by the server.[391]

D. Static code analysis.

1309. Progress could have prevented the Data Breach by strictly analyzing their code for potential security vulnerabilities.[392]

1310. Static code analysis is an industry standard and best practice because it ensures that code is written in a manner that not only provides the expected output, but prevents unexpected or even harmful outputs, such as SQL injection and remote code execution.[393]

---

[388] *Id.*

[389] *Id.*

[390] *Id.*

[391] *Id.*

[392] *Id.*

[393] *Id.*

1311. Analysis of MOVEit Transfer code by a competent developer would have revealed glaring vulnerabilities that could have been removed before the Data Breach, including:

a. Passing unsanitized, unvalidated user input into SQL queries[394]

b. Failing to use parameterized statements to prevent SQL injection[395]

c. Using the BinaryFormatter.Deserialize function[396]

1312. Third-party tools can analyze code for vulnerabilities that may be easy or hard to identify, including SQL injection and deprecated functions.[397]

1313. Progress failed to analyze the MOVEit Transfer code for potential security vulnerabilities, instead blindly relying on outdated, poorly written code that performed as Progress expected under controlled conditions.[398]

E. Vulnerability testing.

1314. Progress could have prevented the Data Breach by testing its code for potential security vulnerabilities, rather than simply using code that performed correctly under controlled conditions.[399]

---

[394] Kinza Yasar, et al., *Definition: SQL injection (SQLi)*, TechTarget (Apr. 2023), https://www.techtarget.com/searchsoftwarequality/definition/SQL-injection.

[395] *Id.*

[396] BinaryFormatter serialization methods are obsolete and prohibited in ASP.NET apps, supra note 77; A8:2017-Insecure Deserialization, supra note 73; OWASP Top 10, supra note 64; pwntester, supra note 82.

[397] Dave Wichers, et al., *Source Code Analysis Tools*, OWASP, https://owasp.org/www-community/Source_Code_Analysis_Tools (last visited Apr. 26, 2024).

[398] *MOVEit Data Breach: Summary and How to Prevent SQL Injection Attacks*, TitanFile, https://www.titanfile.com/blog/moveit-data-breach-summary-and-how-to-prevent-sql-injection-attacks/ (last visited Nov. 26, 2024).

[399] *Id.*

1315. Vulnerability testing is an industry standard and best practice because it subjects code to scrutiny and unexpected user input so that critical flaws can be discovered.[400]

1316. Vulnerability testing involves subjecting software to extreme conditions that may be unexpected in the real world—such as sending improperly formatted requests to incorrect ports—in order to understand how the software reacts and whether any conditions can cause the software to fail or become insecure.[401]

1317. Third-party tools can perform vulnerability testing by engaging in a range of interactions with the software while measuring performance.[402]

1318. Progress failed to analyze the MOVEit Transfer code for potential security vulnerabilities, instead blindly relying on outdated, poorly written code that performed as Progress expected under controlled conditions.[403]

F. External penetration testing.

1319. Progress could have prevented the Data Breach by subjecting their software to penetration testing by a third-party security firm.[404]

1320. Penetration testing is an industry standard and best practice because it subjects code to concerted attack scenarios that test its ability to withstand a data breach.[405]

---

[400] *Id.*

[401] Vitaly Unic, *Vulnerability Testing: Methods, Tools, and 10 Best Practices*, Bright (May 15, 2023), https://brightsec.com/blog/vulnerability-testing-methods-tools-and-10-best-practices/.

[402] *Id.*

[403] *MOVEit Data Breach: Summary and How to Prevent SQL Injection Attacks*, TitanFile, https://www.titanfile.com/blog/moveit-data-breach-summary-and-how-to-prevent-sql-injection-attacks/ (last visited Nov. 26, 2024).

[404] *Id.*

[405] *Id.*

1321. Penetration testing is performed by third-party security firms with expertise in hacking software, whereby the firm attempts to compromise the software using a variety of tactics to test its resilience to an organized attack.[406]

1322. Progress failed to perform adequate penetration testing on MOVEit Transfer, allowing the software to be used without any understanding of its ability to withstand an attempted data breach.[407]

G. Organizations can take steps to mitigate the consequences of an imminent data breach.

1323. When faced with the urgent risk of a breach or data leak by CL0P or similar groups, organizations can take specific steps to address both the immediate threat and longer-term security concerns.

1324. Organizations that maintain sensitive data should have robust and tested incident response plans with clear protocols for handling ransomware and extortion attacks. A plan should include:

a. Detection and isolation: Quickly identify and isolate compromised systems to contain the breach.[408]

b. Monitor dark web threats actively: Organizations can monitor dark web forums for mentions of their data or breaches using threat intelligence tools. This allows for early detection of any data that might be posted and provides a heads-up if attackers begin selling stolen information.[409]

---

[406] *Id.*

[407] *Id.*

[408] *Incident Response Plan (IRP) Basics*, CISA, https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf (last accessed Nov. 24, 2026); Thriveon, *How to Craft an Effective Incident Response Plan*, LinkedIn (Mar. 19, 2024), https://www.linkedin.com/pulse/how-craft-effective-incident-response-plan-thriveon-yyqmc.

[409] Esteban Borges, *Types of Cyber Crime: A Guide to Prevention & Impact*, Recorded Future (June 26, 2024), https://www.recordedfuture.com/threat-intelligence-101/cyber-threats/types-of-cybercrime.

c. Engage in proactive cyber hygiene: Regularly patch systems, enforce strong password policies, and limit access to sensitive data. This can make it harder for groups like CL0P to penetrate systems or spread ransomware.[410]

d. Prepare legal and public relations responses: Immediately involve legal counsel and public relations teams to prepare responses in case data is leaked. This includes engaging with regulators if needed and transparently informing affected stakeholders.[411]

e. Conduct regular tabletop exercises: Practicing breach scenarios with response teams helps ensure readiness to act swiftly, especially if attackers set tight deadlines.[412]

[410] Wiz Experts Team, *Vulnerability Management Best Practices*, WIZ (Sept. 28, 2023), https://www.wiz.io/academy/vulnerability-management-best-practices.

[411] *Data Breach Response: Role of the Legal Team*, Tanner DeWitt (July 6, 2021), https://www.tannerdewitt.com/data-breach-legal-team-external-counsel-privilege/; Daniel Solove, *The Biggest PR Mistake in Privacy and Data Security Incidents: An Interview with PR Expert Melanie Thomas*, LinkedIn (Aug. 11, 2014), https://www.linkedin.com/pulse/20140811174234-2259773-the-biggest-pr-mistake-in-privacy-and-data-security-incidents-an-interview-with-pr-expert-melanie-thomas; *Data Breach Response: A Guide for Business*, FTC (Feb. 2021), https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business.

[412] Ashley Watters, *The Importance of Realistic Tabletop Exercises*, CompTIA (May 7 2024), https://connect.comptia.org/blog/the-importance-of-realistic-tabletop-exercises.

CHAPTER TWO:

FACTUAL ALLEGATIONS AND CAUSES OF ACTION AS AGAINST PROGRESS

I. Progress's culpability for Plaintiffs' and Class Members' losses.

A. Progress knew its software was being used to transfer sensitive information.

1325. Progress knows and intends for MOVEit to be used by its customers to transfer and receive highly sensitive Private Information.

1326. Progress represents itself as "a global supplier of products and services for business applications" that "develops, markets and distributes application development, deployment, integration and management software to business, industry and governments worldwide."[413]

1327. Progress claims "to deliver superior software products and services that empower [its] partners and customers to dramatically improve their development, deployment, integration and management of quality applications worldwide.[414]

1328. Progress specifically advertises and markets MOVEit to potential customers in the following industries: (a) banking and financial services; (b) educational services; (c) healthcare; (d) insurance; (e) manufacturing; (f) public sector; (g) retail; and (h) the United States Federal Government.[415] Indeed, Progress knows that:

a. "Banking, Financial Services and Insurance companies around the globe depend on MOVEit for secure, scalable and compliant file transfer."[416]

---

[413] Progress, SEC Form 10-K (2003), https://www.sec.gov/Archives/edgar/data/876167/000095013503001256/b45503pse10vk.htm.

[414] *Id.*

[415] *MOVEit –Managed File Transfer Software – Use Cases, By Industry*, Progress, https://www.progress.com/moveit (last visited Nov. 26, 2024).

[416] *MOVEit –Managed File Transfer for Banking and Financial Services*, Progress, https://www.progress.com/moveit/banking-and-finance (last visited Nov. 26, 2024).

b. MOVEit is used by "educational institutions of all sizes."[417]

c. "Healthcare organizations around the globe depend on Progress MOVEit managed file transfer to enable more secure, scalable, reliable file sharing to power patient care, business services and help maintain compliance.[418]

d. "MOVEit is the leading secure managed file transfer software that enables online retailers to exchange very sensitive information such as payment information, inventory reports, and other sensitive data quickly and securely across multiple stores and offices."[419]

e. "MOVEit managed file transfer is the leading [managed file transfer] application for federal government file sharing and file security compliance."[420]

1329. Progress is aware and understands that its customers' businesses depend on "transferring mission critical, sensitive data securely and reliably."[421]

1330. Progress markets, advertises, guarantees, and warrants to all its customers that the MOVEit Transfer software will keep Private Information safe and secure from unauthorized access.

1331. Progress promises that MOVEit will "provide a *secure environment* for your most sensitive files, while easily ensuring the reliability of core business processes."[422]

---

[417] *MOVEit –Managed File Transfer for Education*, Progress, https://www.progress.com/moveit/education (last visited Nov. 26, 2024).

[418] *MOVEit –Managed File Transfer for Healthcare*, Progress, https://www.progress.com/moveit/healthcare (last visited Nov. 26, 2024).

[419] *MOVEit – Secure File Transfer for Retail*, Progress, https://www.progress.com/moveit/retail (last visited Nov. 26, 2024).

[420] *MOVEit – FIPS Validated File Transfer Products*, Progress, https://www.progress.com/moveit/government-us-federal-government (last visited Nov. 26, 2024).

[421] *Managed File Transfer Software*, Progress, https://www.progress.com/moveit (last visited Nov. 26, 2024).

[422] *Id.* (emphasis added).

1332. According to Progress: "In a world built on distributed work and collaboration, securing sensitive files is essential. Progress offers file transfer solutions that secure and encrypt your sensitive files, offer new levels of operational efficiency and meet the compliance standards that matter most to your organization."[423]

1333. Progress holds itself out publicly as a trustworthy industry leader worldwide by advertising that customers should "trust Progress for innovation and results" and boasting that "top 10 tech companies rely on Progress," "the 30 largest companies in the world trust Progress," and "70% of Fortune 500 companies trust Progress."[424]

1334. In marketing the MOVEit Transfer software to businesses in a broad range of industries, Progress warrants and promises to customers that MOVEit "makes it easy to choose the exact capabilities that match your organization's specific needs."[425]

1335. Progress promises its clients in the educational services sector that "MOVEit managed file transfer provides easy, secure, automated and compliant movement of PII and other highly sensitive files."[426]

1336. Progress promises its customers in the healthcare industry that it knows "the business of healthcare depends on the reliable, secure and compliant transfer of Protected Health Information (PHI)."

---

[423] *Secure File Transfer – Essential Security for Your Most Important Files*, Progress, https://www.progress.com/file-transfer (last visited Nov. 26, 2024).

[424] *Trust Progress for Innovation and Results*, Progress, https://www.progress.com/ (last visited Nov. 26, 2024).

[425] *MOVEit –Managed File Transfer Software*, Progress, https://www.progress.com/moveit (last visited Nov. 26, 2024).

[426] *MOVEit –Managed File Transfer for Education*, Progress, https://www.progress.com/moveit/education (last visited Nov. 26, 2024).

1337. Progress intended for its customers to rely on its promises and representations that MOVEit would keep Private Information secure from unauthorized access and ensure its customers' compliance with industry standards and regulatory requirements related to data security.

1338. Progress further warrants that MOVEit complies with applicable data security laws and regulations, marketing MOVEit as a tool that will "[e]nsure regulatory compliance in the transfer of PII and Financial Data."[427]

1339. Progress claims "MOVEit enables your organization to meet strict cybersecurity compliance standards such as PCI-DSS, HIPAA, GDPR, SOC2, and more."[428]

1340. Progress warns its clients and potential clients that "[i]ncreasingly strict data protection regulations mandate that networks, user access, databases and business processes are secured to protect financial data and customers' Personally Identifiable Information (PII)."[429] Accordingly, Progress represented that MOVEit would ensure regulatory compliance for customers.

1341. Progress promises its customers in the financial industry that MOVEit will "help[] your organization meet cybersecurity compliance standards such as PCI-DSS, HIPAA, GDPR, SOC2 and more."[430]

---

[427] *See, e.g.*, *MOVEit – Managed File Transfer for Education*, Progress, https://www.progress.com/moveit/education (last visited Nov. 26, 2024).

[428] *MOVEit –Managed File Transfer Software*, Progress, https://www.progress.com/moveit (last visited Nov. 26, 2024).

[429] *MOVEit –Managed File Transfer for Education*, Progress, https://www.progress.com/moveit/education (last visited Nov. 26, 2024).

[430] *MOVEit –Managed File Transfer Software*, Progress, https://www.progress.com/moveit (last visited Nov. 26, 2024).

1342. Progress also recognizes that "[e]ducational institutions need to protect the personally identifiable information (PII) of students, employees, and other stakeholders every day. In addition, valuable intellectual property, health records and other sensitive information require security, visibility, and control that is in line with leading cybersecurity standards such as HIPAA, GDPR, PCI-DSS, and others."[431]

1343. Progress promises its clients in the educational services industry that "[t]he MOVEit suite of Secure Managed File Transfer products assures encryption of external data transfers, delivery to the intended recipient and detailed audit logs. MOVEit provides the security features and flexible deployments that enable you to meet SOX, GLB, PCI and GDPR data protection requirements."[432]

1344. Progress likewise promises its clients in the healthcare industry that "MOVEit provides the features and deployment flexibility required to help healthcare agencies comply with HIPAA, PCI-DSS, GDPR and other leading cybersecurity standards."[433]

1345. Progress warranted that MOVEit would provide protection against the exact dangers and resulting damages it instead exposed and inflicted upon its customers and Plaintiffs.

1346. Progress knew or should have known that the statements and promises it made regarding MOVEit were false and misleading, based on its subpar database development, security procedures, and controls.

---

[431] *MOVEit –Managed File Transfer for Education*, Progress, https://www.progress.com/moveit/education (last visited Nov. 26, 2024).

[432] *MOVEit –Managed File Transfer for Education*, Progress, https://www.progress.com/moveit/education (last visited Nov. 26, 2024).

[433] *MOVEit –Managed File Transfer for Healthcare*, Progress, https://www.progress.com/moveit/healthcare (last visited Nov. 26, 2024).

B. Progress knew of the risks of data breaches and the damage a breach of its software could create.

1347. Progress knows that "[d]ata in motion is data at risk and particular attention must be paid to the security and compliance of [its customers'] external file transfer process."[434]

1348. A data breach is a foreseeable consequence of failing to adequately design and maintain a file transfer application like MOVEit.

1349. Indeed, such consequences have been seen in similar widely publicized breaches involving file transfer solutions like MOVEit—including Accellion FTA and Fortra GoAnywhere MFT.

1350. In the Accellion, Inc. breach, over 100 companies, organizations, universities, and government offices were subject to ransomware attacks as a result of vulnerabilities in its system.

1351. The highly public nature of the Accellion, Inc. breach and similar breaches placed Progress on notice of the foreseeable consequences of its failure to adequately design and maintain its MOVEit applications.

1352. Moreover, the fact that CVE-2023-34362 existed for at least two years prior to the Data Breach indicates that Progress, as the developer of MOVEit, knew or should have known of the vulnerability using reasonably diligent efforts.

1353. Despite adequate notice of the risks associated with its failure to adequately design, maintain, and proactively test the MOVEit application, Progress failed to ensure the security of its platform and ultimately the security of the highly sensitive and confidential Private Information transferred by its customers using MOVEit.

---

[434] *MOVEit –Managed File Transfer for Banking and Financial Services*, Progress, https://www.progress.com/moveit/banking-and-finance (last visited Nov. 26, 2024).

1354. Progress failed to expend the necessary funds to ensure the product it designed, marketed, sold, distributed, and maintained was safe and secure.

1355. As a result, the MOVEit Data Breach created astounding financial repercussions for Progress's customers as well as the many entities and individuals who entrusted Progress's customers with their highly sensitive and confidential Private Information and relied on Progress and Progress's customers to protect and secure that information from unauthorized disclosure.

C. Progress had an obligation to identify and remediate any vulnerabilities in the MOVEit software.

1356. By marketing and advertising MOVEit as a solution for secure transfer and storage of highly sensitive Private Information, Progress assumed legal and equitable duties and knew or should have known it was responsible for:

a. adequately designing, maintaining, and updating its software;

b. promptly detecting, remediating, and notifying its customers of any critical vulnerabilities in its software code;

c. ensuring compliance with industry standards related to data security;

d. ensuring compliance with regulatory requirements related to data security;

e. protecting and securing the Private Information contained in its customers' files from unauthorized disclosure; and

f. providing adequate notice to customers and individuals if their Private Information is disclosed without authorization.

1357. Progress failed to use the requisite degree of care that a reasonably prudent software company would use in designing, developing, and maintaining a secure transfer application software program.

D. Progress knew or should have known of the vulnerabilities in its software and failed to patch them.

1358. SQL injection vulnerabilities, like the one exploited by CL0P in Progress's software, are well-known vulnerabilities that Progress knew or should have known to protect against.

1359. SQL injection vulnerabilities have been listed in the OWASP Top 10 vulnerabilities for many years.[435]

1360. SQL injection vulnerabilities "are caused by software applications that accept data from an untrusted source (internet users), fail to properly validate and sanitize the data, and subsequently use that data to dynamically construct an SQL query to the database backing that application."[436]

1361. Any data that is passed from a user to a vulnerable web application and then processed by the supporting database represents a potential attack vector for SQL injection.[437]

1362. As a software development corporation, Progress was uniquely positioned to prevent SQL injection vulnerabilities.

---

[435] *See, e.g.*, OWASP Top Ten, *Top 10 Web Application Security Risks*, https://owasp.org/www-project-top-ten/ (last visited Nov. 26, 2024); *A03:2021-Injection*, OWASP Top 10: 2021, https://owasp.org/Top10/A03_2021-Injection/ (last visited Nov. 26, 2024); OWASP Top Ten, *2017 Top 10*, https://owasp.org/www-project-top-ten/2017/Top_10 (last visited Nov. 26, 2024); GitHub, https://owasp.org/www-pdf-archive/OWASP_Top_10_-_2013.pdf (last visited Nov. 5, 2024); GitHub, https://owasp.org/www-pdf-archive/OWASP_AppSec_Research_2010_OWASP_Top_10_by_Wichers.pdf (last visited Nov. 5, 2024); GitHub, https://owasp.org/www-pdf-archive/OWASP_Top_10_2007.pdf (last visited Nov. 5, 2024); OWASP Top 10, *Top 10 2004*, https://github.com/owasp-top/owasp-top-2004 (last visited Nov. 5, 2024).

[436] Chad Dougherty, *Practical Identification of SQL Injection Vulnerabilities*, US-Computer Emergency Readiness Team (2012), https://www.cisa.gov/sites/default/files/publications/Practical-SQLi-Identification.pdf

[437] *Id.*

1363. Software developers like Progress are advised to employ parameterized rather than dynamic queries. Parameterized queries are simpler to write and understand and prevent the use of SQL commands inserted by an attacker.

1364. Additional standard practices to prevent SQL injection vulnerabilities include the use of stored procedures, allow-list input validation, application fuzzing, or the use of web application firewalls ("WAFs").

1365. As a software developer, Progress was further in a position to mitigate the risk of SQL injection vulnerabilities by minimizing privileges assigned to each database and employing effective endpoint detection systems.

1366. By failing to adhere to reasonable industry standards related to prevention of SQL injection vulnerabilities, Progress failed to use reasonable care or employ a reasonable industry standard of care for materials that it knew contained Private Information.

1367. Progress's negligent acts and omissions, include, *inter alia*:

a. Negligent design of the MOVEit application;

b. Failure to utilize parameterized inquiries rather than dynamic inquiries;

c. Failure to use stored procedures;

d. Failure to utilize application fuzzing;

e. Failure to use web application firewalls;

f. Failure to conduct regular audits and penetration testing;

g. Failure to document all database accounts, stored procedures, and prepared statements along with their uses;

h. Failure to enforce best practice password and account policies;

i. Failure to use principles of least privilege;

j. Failure to ensure that error messages are generic and do not expose too much information;

k. Failure to sanitize and/or validate input;

l. Failure to deny extended URLs;

m. Failure to disable potentially harmful SQL stored procedure calls;

n. Failure to produce proactive patch production or update and patch production servers with regularity;

o. Failure to adequately secure the application and operation system;

p. Failure to deny unnecessary internet access;

q. Failure to block or restrict internet or intranet access for database systems;

r. Failure to implement firewall rules to block or restrict internet and intranet access or implement firewall rules to block known malicious IP addresses; and

s. Failure to harden internal systems against the potential threat posed by a compromised system against the potential threats poses by a compromised system on their local network.

1368. Progress should have known about the vulnerabilities in the MOVEit software and was negligent in developing, maintaining, and updating the software, because:

a. Progress failed to adhere to basic, well-known industry standards for software security;

b. Progress failed to review and maintain the MOVEit Transfer code to ensure it was secure and met industry standards;

c. Progress allowed its customers to use outdated versions of MOVEit Transfer software;

d. Progress developed and maintained MOVEit Cloud without the vulnerabilities affecting MOVEit Transfer; and

e. Progress knew or should have known the consequences of its failure to follow industry standards for secure software development and maintenance.

1369. Following secure software development practices from the start of development through release and continued maintenance of the software is an industry standard and best practice

because it prevents the possibility of overlooking a critical security vulnerability in outdated code.[438]

1370. Instead of following secure software development practices, Progress instead attempted to maintain and patch its outdated software with critical vulnerabilities, but its maintenance and patch program was ineffective.

1371. As a result of its many design failures, MOVEit was effectively a trojan horse, allowing CL0P unfettered access to the most highly sensitive and confidential data of Progress's customers.

1372. Progress was further negligent in failing to timely detect and remedy the vulnerabilities in the MOVEit Transfer software, despite the fact that the vulnerability now known as CVE-2023-34362 had existed for at least two years prior to the MOVEit Data Breach.

E. Progress's failure to act as quickly as possible led to additional losses.

1373. Progress's delayed disclosure and/or notification of MOVEit's critical security vulnerabilities prevented its customers from taking prompt action, including discontinuing use of MOVEit as a "secure" file transfer application. Moreover, this conduct appears to be ongoing.

1374. Importantly, CVE-2023-34362 was not the only critical vulnerability in MOVEit's code.

1375. In the months following the May 31, 2023, announcement of CVE-2023-34362,[439] Progress disclosed four additional SQL injection vulnerabilities, each of which would also allow a malicious actor to access, modify, and steal data within MOVEit's database. On June 9, 2023,

---

[438] *MOVEit Data Breach: Summary and How to Prevent SQL Injection Attacks*, TitanFile, https://www.titanfile.com/blog/moveit-data-breach-summary-and-how-to-prevent-sql-injection-attacks/ (last visited Nov. 26, 2024).

[439] *CVE-2023-34362 Detail*, NIST, https://nvd.nist.gov/vuln/detail/CVE-2023-34362 (last updated Nov. 21, 2024).

Progress announced SQL injection vulnerability CVE-2023-35036.[440] On June 15, 2023, Progress announced yet another SQL injection vulnerability, CVE-2023-35708.[441] And on July 7, 2023, Progress released a service pack that addressed three additional vulnerabilities, including two SQL injection vulnerabilities: CVE-2023-36934[442]and CVE-2023-36932.[443] The third, CVE-2023-36933,[444] would allow an attacker to trigger the application to terminate.

1376. All six of the vulnerabilities, disclosed over a period of two months between May 31, 2023, and July 7, 2023, were ranked as "high" or "critical." In all cases, the original vulnerability could be exploited to upload a web shell onto the MOVEit Transfer server. The web shell allowed threat actors to enumerate files and folders on the MOVEit Transfer server, read configuration information, download files, and create or delete MOVEit server user accounts.[445]

1377. Similarly, on September 27, 2023, cybersecurity researchers announced a maximum severity remote code execution vulnerability in Progress's WS_FTP file share platform.

---

[440] *CVE-2023-35036 Detail*, NIST, https://nvd.nist.gov/vuln/detail/CVE-2023-35036 (last updated Nov. 21, 2024).

[441] *CVE-2023-35708 Detail*, NIST, https://nvd.nist.gov/vuln/detail/CVE-2023-35708 (last updated Nov. 21, 2024).

[442] *CVE-2023-36934 Detail*, NIST, https://nvd.nist.gov/vuln/detail/CVE-2023-36934 (last updated Nov. 21, 2024) (CVE-2023-36934 is a critical, unauthenticated SQL injection vulnerability).

[443] *CVE-2023-36932 Detail*, NIST, https://nvd.nist.gov/vuln/detail/CVE-2023-36932 (last updated Nov. 21, 2024) (CVE-2023-36932 is a high-severity SQL injection vulnerability that could allow authenticated attackers to gain access to the MOVEit Transfer database).

[444] *CVE-2023-36933 Detail*, NIST, https://nvd.nist.gov/vuln/detail/CVE-2023-36933 (last updated Nov. 21, 2024) (CVE-2023-36933 is an exception handling issue that could allow an attacker to crash the application).

[445] Threat Brief – MOVEit Transfer SQL Injection Vulnerabilities: CVE-2023-34362, CVE-2023-35036 and CVE-2023-34362, CVE-2023-35036 and CVE-2023-35708 (Updated Oct. 4), Unit 42, https://unit42.paloaltonetworks.com/threat-brief-moveit-cve-2023-34362/ (last updated Oct. 4, 2023).

This vulnerability, CVE-2023-40044, a .NET deserialization vulnerability, allows threat actors to remotely execute commands on its operating with a simple HTTP request.

1378. On September 30, 2023, cybersecurity company Rapid7 announced that it had observed multiple instances of threat actors exploiting CVE-2023-40044.

1379. On October 2, 2023—days after the CVE-2023-40044 vulnerability was disclosed by a third party, Progress responded by blaming security researchers for the failures of its code, announcing that it was "disappointed" that security researchers had "provided threat actors a roadmap on how to exploit the vulnerabilities" that Progress itself had created and failed to remedy.[446]

1380. Rather than take responsibility for the vulnerability and their lack of disclosure, Progress blamed those who sought to inform Progress's customers. This is particularly concerning given that the MOVEit SQL injection vulnerability CVE-2023-34362 had existed for two years prior to the MOVEit Data Breach.

1381. According to Kroll, a "forensic review [] also identified activity indicating that the Cl0p threat actors were likely experimenting with ways to exploit this particular vulnerability as far back as 2021."[447] Other reliable cybersecurity firms have also concluded that this vulnerability was present at least as early as 2021.[448]

---

[446] Sergiu Gatlan, *Exploit available for critical WS_FTP bug exploited in attacks*, BleepingComputer (Oct. 2, 2023, 1:11 PM), https://www.bleepingcomputer.com/news/security/exploit-available-for-critical-ws-ftp-bug-exploited-in-attacks/.

[447] Scott Downie, et al., *Cl0p Ransomware Likely Sitting on MOVEit Transfer Vulnerability (CVE-2023-34362) Since 2021*, Kroll (June 8, 2023), https://www.kroll.com/en/insights/publications/cyber/clop-ransomware-moveit-transfer-vulnerability-cve-2023-34362.

[448] *See* Chris Swagler, *MOVEit Data Breach: Lessons in Application Security for Modern Businesses*, Speartip (Sept. 27, 2023), https://www.speartip.com/moveit-data-breach-application-security/.

1382. Once the first vulnerability was discovered by Progress in May of 2023, Progress should have initiated an evaluation of all its software for vulnerabilities. Likewise, Progress's announcement of the first vulnerability on May 31, 2023, should have triggered Defendants to begin taking security measures.

1383. As a direct and proximate consequence of Progress's misconduct, acts, and omissions, Progress's customers have experienced direct monetary damages, including, but not limited to: costs associated with ransomware payments, legal fees associated with incident response and regulatory concerns, costs associated with data breach response and forensic investigation, and costs associated with breach remediation and settlement of consumer claims.

1384. As a direct and proximate consequence of Progress's misconduct, acts, and omissions, Progress's customers' users, including Plaintiffs and Class Members in these actions, have experienced direct and indirect monetary damages and other harm as described herein.

1385. For the reasons set forth in detail above, Progress is directly liable to every member of every proposed class and faces substantial exposure—both individually and via joint and several liability—as a primary defendant in the claims stemming from the MOVEit vulnerability. Upon information and belief, Progress is able to satisfy actual or potential judgments on behalf of the proposed classes. Progress further faces actual and potential indemnification/contribution claims from its co-defendants and customers.

II. CLASS ALLEGATIONS AGAINST PROGRESS

1386. Plaintiffs Keith Bailey, Gregory Bloch, Karen Boginski, Camille Burgan, Eugene Burgan, Doris Cadet, Steven Checchia, Amanda Copans, Barbara Cruciata, Ben Dieck, Victor DiLuigi, Marvin Dovberg, Deanna Duarte, Laquesha George, Michelle Gonsalves, Gilbert Hale, Lynda Hale, Brinitha Harris, Patrice Hauser, Tricia Hernandez, Margaret Kavanagh, Aunali Khaku, Patricia Marshall, Shellie McCaskell, Megan McClendon, Elaine McCoy, John Meeks,

Terrill Mendler, Manuel Mendoza, Denise Meyer, Ricardo Moralez, Rita Pasquarelli, Margaret Phelan, Rob Plotke, Hannah Polikowsky, Christopher Rehm, Jvanne Rhodes, Diamond Roberts, Taneisha Robertson, Sherrie Rodda, Aldreamer Smith, Jose Soto, Alexys Taylor, Steven Teppler, Yvette Tillman, Katharine Uhrich, Jeff Weaver, and Tamara Williams bring the causes of action listed below on behalf of themselves and, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) as representatives of the following proposed Progress Class:

a. Progress Nationwide Class: All persons whose Private Information was compromised in the MOVEit data breach.

1387. Plaintiffs also bring this cause of action on behalf of themselves and on behalf of the following Progress State Classes:

a. Progress California Class: All residents of California whose Private Information was compromised in the MOVEit data breach.

b. Progress California PHI Class: All residents of California whose PHI was compromised in the MOVEit data breach.

c. Progress Connecticut Class: All residents of Connecticut whose Private Information was compromised in the MOVEit data breach.

d. Progress Florida Class: All residents of Florida whose Private Information was compromised in the MOVEit data breach.

e. Progress Georgia Class: All residents of Georgia whose Private Information was compromised in the MOVEit data breach.

f. Progress Illinois Class: All residents of Illinois whose Private Information was compromised in the MOVEit data breach.

g. Progress Iowa Class: All residents of Iowa whose Private Information was compromised in the MOVEit data breach.

h. Progress Indiana Class: All residents of Indiana whose Private Information was compromised in the MOVEit data breach.

i. Progress Michigan Class: All residents of Michigan whose Private Information was compromised in the MOVEit data breach.

j. Progress Nebraska Class: All residents of Nebraska whose Private Information was compromised in the MOVEit data breach.

k. Progress New Jersey Class: All residents of New Jersey whose Private Information was compromised in the MOVEit data breach.

l. Progress New York Class: All residents of New York whose Private Information was compromised in the MOVEit data breach.

m. Progress North Carolina Class: All residents of North Carolina whose Private Information was compromised in the MOVEit data breach.

n. Progress Ohio Class: All residents of Ohio whose Private Information was compromised in the MOVEit data breach.

o. Progress Pennsylvania Class: All residents of Pennsylvania whose Private Information was compromised in the MOVEit data breach.

p. Progress South Carolina Class: All residents of South Carolina whose Private Information was compromised in the MOVEit data breach.

q. Progress Tennessee Class: All residents of Tennessee whose Private Information was compromised in the MOVEit data breach.

r. Progress Texas Class: All residents of Texas whose Private Information was compromised in the MOVEit data breach.

s. Progress Vermont Class: All residents of Vermont whose Private Information was compromised in the MOVEit data breach.

t. Progress Washington Subclass: All residents of Washington whose Private Information was compromised in the MOVEit data breach.

The foregoing state-specific Progress Classes are collectively referred to as the "Progress State Classes." All of the foregoing Classes are referred to herein, collectively, as the "Progress Bellwether Class." Excluded from the Progress Bellwether Class are: (1) the judges presiding over the action, Class Counsel, and members of their families; (2) the Defendants, their subsidiaries, parent companies, successors, predecessors, and any entity in which Defendants or their parents have a controlling interest, and their current or former officers and directors; (3) persons who properly opt out; and (4) the successors or assigns of any such excluded persons.

1388. **Numerosity:** Progress Bellwether Class Members are so numerous that their individual joinder is impracticable, as the proposed Progress Bellwether Class includes at least 85 million[449] members who are geographically dispersed.

1389. **Typicality:** Bellwether Plaintiffs' claims are typical of Progress Bellwether Class Members' claims. Bellwether Plaintiffs and all Progress Bellwether Class Members were injured through Progress's uniform misconduct, and Bellwether Plaintiffs' claims are identical to the claims of the Progress Bellwether Class Members they seek to represent.

1390. **Adequacy**: Bellwether Plaintiffs' interests are aligned with the Progress Bellwether Class Members they seek to represent, and Bellwether Plaintiffs have retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Bellwether Plaintiffs and their counsel intend to prosecute this action vigorously. The Progress Bellwether Class's interests are well-represented by Bellwether Plaintiffs and undersigned counsel.

1391. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Bellwether Plaintiffs' and Progress Bellwether Class Members' claims. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for class members individually to effectively redress Progress's wrongdoing. Even if class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system,

[449] Bert Kondruss, *MOVEit hack victim list*, Kon Briefing, https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html (last updated Dec. 20, 2023).

presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

1392. **Commonality and Predominance**: The following questions common to all Progress Bellwether Class Members predominate over any potential questions affecting individual Progress Bellwether Class Members:

a. Whether Progress had a duty to implement and maintain reasonable security procedures and practices to protect and secure Bellwether Plaintiffs' and Progress Bellwether Class Members' Private Information from unauthorized access and disclosure;

b. Whether Progress failed to exercise reasonable care to secure and safeguard Bellwether Plaintiffs' and Progress Bellwether Class Members' Private Information;

c. Whether Progress breached their duties to protect Bellwether Plaintiffs' and Progress Bellwether Class Members' Private Information;

d. Whether Progress violated the statutes alleged herein;

e. Whether Bellwether Plaintiffs and all other Progress Bellwether Class Members are entitled to damages and the measure of such damages and relief.

1393. Given that Progress engaged in a common course of conduct as to Bellwether Plaintiffs and Progress Bellwether Class Members, similar or identical injuries and common law violations are involved, and common questions outweigh any potential individual questions.

III. CAUSES OF ACTION AGAINST PROGRESS

PROGRESS BELLWETHER FIRST CLAIM FOR RELIEF
Negligence

(Brought by Plaintiffs on behalf of the Progress Nationwide Class, or, in the alternative, Progress State Classes, against Progress)

1394. Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1395. All Bellwether Plaintiffs bring this claim against Progress on behalf of the Progress Nationwide Class or, in the alternative, the Progress State Classes.

1396. Entities using Progress's MOVEit software require their customers to submit non-public Private Information as a condition of becoming a customer and receiving services.

1397. Through its relationships with these entities, Progress facilitated the transfer and storage of the Private Information of Plaintiffs and Progress Bellwether Class Members as part of its business, which affects commerce.

1398. As customers of entities using Progress's MOVEit software, Plaintiffs and Progress Bellwether Class Members, or their service providers, continue to send these entities new Private Information as they continue to receive services or conduct business with these entities.

1399. Plaintiffs and Progress Bellwether Class Members entrusted entities using Progress's MOVEit software with their Private Information with the reasonable understanding that their highly personal Private Information would be safeguarded and protected against unauthorized disclosure.

1400. Progress had full knowledge of the high monetary value and sensitivity of Plaintiffs' and Progress Bellwether Class Members' Private Information and the types of harm that

Plaintiffs and Progress Bellwether Class Members could and would suffer if their Private Information was wrongfully disclosed.

1401. By assuming the responsibility to transfer and store this data through its MOVEit software, in order to derive business value and commercial profits, Progress assumed a duty under common law to Plaintiffs and Progress Bellwether Class Members to exercise reasonable care to ensure that its MOVEit software would secure and safeguard their Private Information and keep it from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

1402. Progress owed a duty of care to Plaintiffs and Progress Bellwether Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

1403. Progress's duty to use reasonable care arose from several sources, including, but not limited to, those described below.

1404. Progress holds itself out as a trusted provider of secure file-transfer software. Its duty to develop software that included reasonable security measures arose as a result of the special relationship that existed between Progress, on the one hand, and Plaintiffs and Progress Bellwether Class Members, through their relationship with users of MOVEit software, on the other hand. That special relationship arose because of Progress's business as the developer of MOVEit, which required Plaintiffs and Progress Bellwether Class Members to provide and entrust users of MOVEit software with their confidential Private Information, who in turn relied on Progress's MOVEit software to transfer and store that data securely.

1405. Thus, Progress was in a unique and superior position to protect against the harm suffered by Plaintiffs and Progress Bellwether Class Members as a result of the Data Breach.

1406. Progress owed a duty to Plaintiffs and Progress Bellwether Class Members to develop and maintain a software file transfer service that employed reasonable data security measures to protect their customers' Private Information.

1407. The risk that unauthorized persons would attempt to gain access to Plaintiffs' and Progress Bellwether Class Members' Private Information and misuse was foreseeable to Progress. It had a common law duty to prevent foreseeable harm to others because Plaintiffs and Progress Bellwether Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Progress. By collecting, receiving, storing, and using Private Information that is routinely targeted by criminals for unauthorized access, Progress was obligated to act with reasonable care to protect against these foreseeable threats.

1408. Given that Progress collects, stores, and uses vast amounts of Private Information and the high market value of this data, it was inevitable that unauthorized cybercriminals would at some point try to access Progress's computer networks. Progress knew, or should have known, the importance of exercising reasonable care in handling the Private Information entrusted to them.

1409. Because Progress's business pertains to Private Information, Progress's Privacy Policies acknowledge its legal obligations under HIPAA as well as its duty to protect and prevent from disclosure all other data it collects and stores.

1410. Progress had a duty to promptly and adequately notify Plaintiffs and Progress Bellwether Class Members about the Data Breach, but failed to do so, and breached this duty.

1411. Progress had and continues to have duties to adequately disclose that Plaintiffs' and Progress Bellwether Class Members' Private Information might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was and continues to be necessary to allow Plaintiffs and the Progress Bellwether Class Members

to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

1412. Progress breached its duties owed to Plaintiffs and Progress Bellwether Class Members and thus was negligent. Progress breached these duties by, among other things: (a) mismanaging its software development and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of its MOVEit transfer software, which resulted in the unauthorized access and compromise of Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to detect the breach at the time it began or within a reasonable time thereafter; and (f) failing to follow its own policies and practices published to its clients.

1413. Plaintiffs and Progress Bellwether Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach and harms suffered.

1414. Progress's negligent conduct is ongoing, in that Plaintiffs' and Progress Bellwether Class Members' Private Information remains stored on Progress's MOVEit software in an unsafe and insecure manner.

1415. Plaintiffs and Progress Bellwether Class Members are entitled to injunctive relief requiring Progress to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Progress Bellwether Class Members.

PROGRESS BELLWETHER SECOND CLAIM FOR RELIEF
Negligence Per Se
(Brought by Plaintiffs on behalf of the Progress Nationwide Class, or, in the alternative, Progress State Classes, against Progress)

1416. Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two

1417. All Bellwether Plaintiffs bring this claim against Progress on behalf of the Progress Nationwide Class or, in the alternative, the Progress State Classes.

1418. Progress had duties arising under HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and the FTC Act to protect Plaintiffs' and Progress Bellwether Class Members' Private Information.

1419. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Progress, of failing to use reasonable measures to protect sensitive consumer data, including Private Information.

1420. Various FTC publications and orders promulgated pursuant to the FTC Act also form the basis of Progress's duty.

1421. Progress breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to implement fair, reasonable, or appropriate computer systems and data security practices that complied with applicable industry standards to safeguard Plaintiffs' and Progress Bellwether Class Members' Private Information as part of its business practices.

1422. Many entities that use MOVEit are "covered entities" under HIPAA, and Progress is a "business associate."

1423. As a business associate, Progress owed legal obligations to implement administrative, technical, and physical safeguards. 42 U.S.C. § 17931 (applying security requirements to business associates and incorporating security requirements into BAAs between business associates and covered entities); *see also* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards); 42 U.S.C. § 17902.[450]

1424. Progress's specific negligent acts and omissions, resulting in failure to comply with HIPAA and HITECH regulations include, but are not limited to, the following: (i) failing to adopt, implement, and maintain adequate security measures to safeguard Progress Bellwether Class Members' Private Information; (ii) failing to adequately monitor the security of its MOVEit software; (iii) allowing unauthorized access to Progress Bellwether Class Members' Private Information; (iv) failing to detect in a timely manner that Progress Bellwether Class Members' Private Information had been compromised; and (v) failing to timely and adequately notify Progress Bellwether Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

1425. Progress's violations of HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and Section 5 of the FTC Act (and similar state statutes) independently constitute negligence *per se*.

1426. Plaintiffs and Progress Bellwether Class Members are consumers within the class of persons that HIPAA, HITECH, and Section 5 of the FTC Act were intended to protect.

[450] *HITECH Act Summary*, HIPAA Survival Guide, https://perma.cc/HSQ6-4942 (last accessed Nov. 27, 2024).

1427. The harms that have occurred are the types of harm HIPAA, HITECH, and the FTC Act were intended to guard against.

1428. The FTC has pursued enforcement actions against businesses and healthcare entities that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harms as those suffered by Plaintiffs and the Progress Bellwether Class.

1429. In addition, under various state data security and consumer protection statutes such as those outlined herein, Progress had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Progress Bellwether Class Members' Private Information.

1430. Progress's conduct was particularly unreasonable given the nature and amount of Private Information that its MOVEit software transferred and stored, the high frequency of cyber-attacks that target the exact type of Private Information targeted here, and the foreseeable consequences of a data breach of that nature.

1431. Plaintiffs and Progress Bellwether Class Members were foreseeable victims of Progress's violations of HIPAA, HITECH, and the FTC Act, and state data security and consumer protection statutes. Progress knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiffs' and Progress Bellwether Class Members' Private Information would cause damage to Plaintiffs and the Progress Bellwether Class.

1432. Plaintiffs and Progress Bellwether Class Members were foreseeable victims of Progress's negligent acts and omissions. Progress knew or should have known that its failure to implement reasonable data security measures to protect and safeguard information transferred and

stored on the MOVEit platform, i.e., Plaintiffs' and Progress Bellwether Class Members' Private Information, would cause damage to Plaintiffs and the Progress Bellwether Class.

1433. Progress violated its own policies by failing to maintain the confidentiality of Plaintiffs' and Progress Bellwether Class Members' records; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Progress Bellwether Class Members' PHI, and ultimately disclosing Plaintiffs' and Progress Bellwether Class Members' PHI.

1434. Progress violated its Business Associate Agreements ("BAA") with covered entities, under which it agreed to protect customers' PHI, including the PHI of Plaintiffs and Progress Bellwether Class Members, and under which it was subject to privacy and security safeguard requirements and standards established by HIPAA, HITECH, and the Omnibus Rule.

1435. But for Progress's violations of the applicable laws and regulations, Plaintiffs' and Progress Bellwether Class Members' Private Information would not have been accessed by unauthorized parties.

1436. As a direct and proximate result of Progress's negligence *per se*, Plaintiffs and Progress Bellwether Class Members have suffered and will continue to suffer injuries, including, but not limited to: (i) theft of their Private Information; (ii) costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts; (iii) costs associated with purchasing credit monitoring and identity theft protection services; (iv) lowered credit scores resulting from credit inquiries following fraudulent activities; (v) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Progress's Data Breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft

protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts; (vi) the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals; (vii) damages to and diminution in value of their Private Information entrusted indirectly to Progress with the mutual understanding that it would safeguard Plaintiffs' and Progress Bellwether Class Members' data against theft and not allow access and misuse of their data by others; (viii) continued and certainly increased risk of exposure to hackers and thieves of their Private Information, and additional unauthorized viewing of their Private Information that was already hacked in the Data Breach; (ix) loss of their privacy and confidentiality in their Private Information; (x) loss of personal time and opportunity costs to monitor and/or remedy harms caused by theft of their Private Information; (xi); an increase in spam calls, texts, and/or emails; and (xii) the continued and certainly increased risk to their Private Information.

1437. As a direct and proximate result of Progress's negligence *per se*, Plaintiffs and the Progress Bellwether Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

1438. Finally, as a direct and proximate result of Progress's negligence *per se*, Plaintiffs and the Progress Bellwether Class have suffered and will suffer the continued risks of exposure of their Private Information, which remains on Progress's MOVEit software and is subject to further unauthorized disclosures so long as Progress fail to undertake appropriate and adequate measures to protect the Private Information via improved security measures.

PROGRESS BELLWETHER THIRD CLAIM FOR RELIEF
Breach of Third-Party Beneficiary Contract
(Brought by Plaintiffs on behalf of the Progress Nationwide Class, or, in the alternative, Progress State Classes, against Progress)

1439. Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two

1440. All Bellwether Plaintiffs bring this claim against Progress on behalf of the Progress Nationwide Class or, in the alternative, the Progress State Classes.

1441. Upon information and belief, Progress entered into contracts with various direct users, vendors, vendor contracting entities, and vendor contracting entity customers to provide secure file transfer services, servers, and/or related equipment and services that included access to and use of the MOVEit software, data security practices, procedures, and protocols related to the MOVEit software sufficient to safeguard the Plaintiffs' and Progress Bellwether Class Members' Private Information that was entrusted to these various entities.

1442. Upon information and belief, contracts between Progress and its direct or indirect customers were made expressly for the benefit of the individuals whose data was transferred and stored on MOVEit software as a result of those contracts, as it was their Private Information that Progress agreed to receive, store, utilize, transfer, and protect through its services, so that Progress's customers could directly or indirectly provide them with goods and services. Thus, the benefit of collection, use, and protection of the Private Information belonging to Plaintiffs and Progress Bellwether Class Members was the direct and primary objective of the contracting parties, and Plaintiffs and Progress Bellwether Class Members were direct and express beneficiaries of such contracts.

1443. Progress and its direct or indirect customers knew or should have known that if they were to breach these contracts, Plaintiffs and Progress Bellwether Class Members would be harmed.

1444. Progress and its direct or indirect customers breached their contracts by, among other things, failing to adequately secure Plaintiffs' and Progress Bellwether Class Members' Private Information, and, as a result, Plaintiffs and Progress Bellwether Class Members were harmed.

1445. As a direct and proximate result of Progress's and its direct or indirect customers' breach, Plaintiffs and Progress Bellwether Class Members are at a current and ongoing risk of identity theft, and have already sustained incidental and consequential damages including: (i) financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out-of-pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their Private Information; (vii) future costs of identity theft monitoring; and (viii) the continued risk to their Private Information, which remains in Progress's and its direct or indirect customers' control, and which is subject to further breaches, so long as Progress and its direct or indirect customers fail to undertake appropriate and adequate measures to protect Plaintiffs' and Progress Bellwether Class Members' Private Information.

1446. Plaintiffs and Progress Bellwether Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

PROGRESS BELLWETHER FOURTH CLAIM FOR RELIEF
Unjust Enrichment
(Brought by Plaintiffs on behalf of the Progress Nationwide Class, or, in the alternative, Progress State Classes, against Progress)

1447. Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1448. All Bellwether Plaintiffs bring this claim against Progress on behalf of the Progress Nationwide Class or, in the alternative, the Progress State Classes.

1449. Plaintiffs and Progress Bellwether Class Members conferred a monetary benefit on the direct users, vendors, vendor contracting entities, and vendor contractor entity customers who utilized MOVEit software in connection with obtaining services, specifically providing them with their Private Information. In exchange, Plaintiffs and Progress Bellwether Class Members should have received the services or benefits that were the subject of the transaction, and should have had their Private Information protected with adequate data security.

1450. The direct users, vendors, vendor contracting entities, and vendor contractor entity customers who utilized MOVEit software would be unable to engage in their regular course of business without that Private Information and they accepted the monetary benefits Plaintiffs and Progress Bellwether Class Members provided.

1451. Plaintiffs and Progress Bellwether Class Members also conferred a monetary benefit indirectly to Progress via Progress's relationship with users of MOVEit software who used MOVEit software to store or transfer Plaintiffs' and Progress Bellwether Class Members' Private Information. Progress would be unable to engage in its regular course of business without that Private Information, and it accepted the monetary benefits from the provision of Plaintiffs' and Progress Bellwether Class Members' Private Information.

1452. Progress knew that Plaintiffs and Progress Bellwether Class Members conferred a benefit upon it and accepted and retained those benefits by allowing users of MOVEit software to accept, retain, and use the Private Information entrusted to them through the MOVEit software. Progress profited from Plaintiffs' retained data and used Plaintiffs' and Progress Bellwether Class Members' Private Information for business purposes.

1453. Acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Progress to retain that benefit without payment of the value thereof. Specifically, Progress enriched itself by saving the costs it reasonably should have expended on data security measures to secure its MOVEit software and thereby secure Plaintiffs' and Progress Bellwether Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Progress instead calculated to increase its own profit at the expense of Plaintiffs and Progress Bellwether Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Progress Bellwether Class Members, on the other hand, suffered as a direct and proximate result of Progress's decisions to prioritize its own profit over the requisite data security.

1454. Progress failed to secure Plaintiffs' and Progress Bellwether Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Progress Bellwether Class Members for the value that their Private Information provided.

1455. Because Progress failed to implement appropriate data management and security measures, under the principles of equity and good conscience, it would be unjust if Progress were permitted to retain the monetary benefit belonging to Plaintiffs and Progress Bellwether Class Members.

1456. Progress acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

1457. If Plaintiffs and Progress Bellwether Class Members had known that Progress had not secured the MOVEit software responsible for transferring or storing their Private Information, they would not have agreed to provide their Private Information to the direct users, vendors, vendor contracting entities, and vendor contractor entity customers who utilized MOVEit software.

1458. Had Plaintiffs and Progress Bellwether Class Members known that Progress did not and would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would not have entrusted their Private Information to the direct users, vendors, vendor contracting entities, and vendor contractor entity customers who utilized MOVEit software.

1459. As a direct and proximate result of Progress's conduct, Plaintiffs and Progress Bellwether Class Members have suffered or will suffer injury, including, but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to determine for themselves how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information and diminution of its value; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains on Progress's software and is subject to further unauthorized disclosures so long as Progress fail to undertake appropriate and adequate measures to protect Private Information kept on MOVEit software; (vii) future costs in

terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Progress Bellwether Class Members; (viii) emotional distress, anxiety, and inconvenience; (ix) irreparable breach of confidence in their insurance providers; and (x) loss of benefit of the bargain (price premium damages in the form of overpayment for dental insurance).

1460. As a direct and proximate result of Progress's conduct, Plaintiffs and Progress Bellwether Class Members have suffered and will continue to suffer other forms of injury and/or harm. It would be inequitable for Progress to retain the benefits without paying fair value for them.

1461. Plaintiffs and Progress Bellwether Class Members are entitled to restitution and/or damages from Progress and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Progress from its wrongful conduct, as well as return of their sensitive Private Information and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Progress Bellwether Class Members may seek restitution or compensation.

1462. Plaintiffs and Progress Bellwether Class Members may not have an adequate remedy at law against Progress, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

PROGRESS BELLWETHER FIFTH CLAIM FOR RELIEF
Bailment
(Brought by Plaintiffs on behalf of the Progress Nationwide Class, or, in the alternative, Progress State Classes, against Progress)

1463. Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1464. All Bellwether Plaintiffs bring this claim against Progress on behalf of the Progress Nationwide Class or, in the alternative, the Progress State Classes.

1465. Plaintiffs and Progress Bellwether Class Members indirectly provided Private Information to Progress, and Progress was under a duty to keep that Information private and confidential.

1466. Progress received this Private Information from Plaintiffs and Progress Bellwether Class Members through the direct users, vendors, vendor contracting entities, and vendor contractor entity customers who utilized MOVEit software.

1467. Plaintiffs' and Progress Bellwether Class Members' Private Information is personal property and was conveyed to Progress for the certain purpose of keeping the Information private and confidential.

1468. Plaintiffs' and Progress Bellwether Class Members' Private Information has value and is highly prized by hackers and criminals. Progress was aware of the risks it took when accepting the Private Information for safeguarding and assumed the risk voluntarily.

1469. Once Progress accepted Plaintiffs' and Progress Bellwether Class Members' Private Information, it was in the exclusive possession of that Information, and neither Plaintiffs nor Progress Bellwether Class Members could control that information once it was within the possession, custody, and control of Progress.

1470. Progress did not safeguard Plaintiffs' or Progress Bellwether Class Members' Private Information when it failed to adopt and enforce adequate security safeguards to prevent the known risk of a cyberattack.

1471. Progress's failure to safeguard Plaintiffs' and Progress Bellwether Class Members' Private Information resulted in that Information being accessed or obtained by third-party cybercriminals.

1472. As a result of Progress's failure to keep Plaintiffs' and Progress Bellwether Class Members' Private Information secure, Plaintiffs and Progress Bellwether Class Members suffered injury, for which compensation— including nominal damages and compensatory damages—are appropriate.

PROGRESS BELLWETHER SIXTH CLAIM FOR RELIEF
Invasion of Privacy (Intrusion upon Seclusion)
(Brought by Plaintiffs on behalf of the Progress Nationwide Class, or, in the alternative, Progress State Classes, against Progress)

1473. Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1474. All Bellwether Plaintiffs bring this claim against Progress on behalf of the Progress Nationwide Class or, in the alternative, the Progress State Classes.

1475. Plaintiffs and Progress Bellwether Class Members had a reasonable expectation of privacy in the Private Information that Progress failed to safeguard and allowed to be accessed by way of the Data Breach.

1476. Progress's conduct as alleged above intruded upon Plaintiffs' and Progress Bellwether Class Members' seclusion under common law.

1477. By intentionally and/or knowingly failing to keep Plaintiffs' and Progress Bellwether Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Progress intentionally invaded Plaintiffs' and Progress Bellwether Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs' and Progress Bellwether Class Members' private affairs in a manner that identifies Plaintiffs and Progress Bellwether Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiffs and Progress Bellwether Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiffs and Progress Bellwether Class Members.

1478. Progress knew that an ordinary person in Plaintiffs' and Progress Bellwether Class Members' positions would consider Progress's intentional actions highly offensive and objectionable.

1479. Progress invaded Plaintiffs' and Progress Bellwether Class Members' right to privacy and intruded into Plaintiffs' and Progress Bellwether Class Members' seclusion by intentionally failing to safeguard, misusing, and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

1480. Progress intentionally concealed from Plaintiffs and Progress Bellwether Class Members an incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

1481. As a proximate result of such intentional misuse and disclosures, Plaintiffs' and Progress Bellwether Class Members' reasonable expectations of privacy in their Private Information were unduly frustrated and thwarted. Progress's conduct, amounting to a substantial and serious invasion of Plaintiffs' and Progress Bellwether Class Members' protected privacy interests, caused anguish and suffering such that an ordinary person would consider Progress's intentional actions or inaction highly offensive and objectionable.

1482. In failing to protect Plaintiffs' and Progress Bellwether Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Progress

acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Progress Bellwether Class Members' rights to have such Information kept confidential and private.

1483. As a direct and proximate result of the foregoing conduct, Plaintiffs seek an award of damages on behalf of themselves and the Progress Bellwether Class Members.

PROGRESS BELLWETHER SEVENTH CLAIM FOR RELIEF
Invasion of Privacy (Public Disclosure of Private Facts)
(Brought by Plaintiffs on behalf of the Progress Nationwide Class, or, in the alternative, Progress State Classes, against Progress)

1484. Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1485. All Bellwether Plaintiffs bring this claim against Progress on behalf of the Progress Nationwide Class or, in the alternative, the Progress State Classes.

1486. Plaintiffs and Progress Bellwether Class Members reasonably expected that the highly personal, sensitive Private Information entrusted to Progress indirectly would be kept private, confidential, and secure and would not be disclosed to any unauthorized third party or for any improper purpose.

1487. Progress unlawfully invaded the privacy rights of Plaintiffs and Progress Bellwether Class Members by:

a. Failing to adequately secure their sensitive Private Information from disclosure to unauthorized third parties or for improper purposes;

b. Enabling the disclosure of personal and sensitive facts and information about them in a manner highly offensive to a reasonable person; and

c. Enabling the disclosure of their personal and sensitive Private Information without their informed, voluntary, affirmative, and clear consent.

1488. Plaintiffs' and Progress Bellwether Class Members' Private Information that was publicized due to the Data Breach, such as health information and Social Security numbers, was

highly sensitive, private, confidential, and of no general public interest, and a reasonable person would consider its publication highly offensive and egregious.

1489. A reasonable person would find it highly offensive that Progress, having collected Plaintiffs' and Progress Bellwether Class Members' sensitive Private Information indirectly in a commercial transaction, failed to protect such Private Information from unauthorized disclosure to third parties.

1490. In failing to adequately protect Plaintiffs' and Progress Bellwether Class Members' sensitive Private Information, Progress acted in reckless disregard of Plaintiffs' and Progress Bellwether Class Members' privacy rights. Progress knew or should have known of the risks of failing to implement adequate data security practices and the foreseeability and offensiveness of such disclosures.

1491. Progress violated Plaintiffs' and Progress Bellwether Class Members' right to privacy under common law.

1492. Progress's unlawful invasions of privacy damaged Plaintiffs and Progress Bellwether Class Members. As a direct and proximate result of Progress's unlawful invasion of privacy and public disclosure of private facts, Plaintiffs and Progress Bellwether Class Members' reasonable expectations of privacy were frustrated and defeated. Plaintiffs and Progress Bellwether Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out-of-pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution

of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains on Progress's software, and is subject to further breaches, so long as Progress fail to undertake appropriate and adequate measures to protect Plaintiffs' and Progress Bellwether Class Members' Private Information.

1493. Plaintiffs and Progress Bellwether Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach and these invasions of privacy.

1494. Plaintiffs and Progress Bellwether Class Members are also entitled to injunctive relief requiring Progress to, inter alia: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to Plaintiffs and Progress Bellwether Class Members.

PROGRESS BELLWETHER EIGHTH CLAIM FOR RELIEF
Massachusetts General Laws, Chapter 93A
M.G.L. ch. 93A §§ 2 and 9
(Brought by Plaintiffs on behalf of the Progress Nationwide Class, or, in the alternative, Progress State Classes, against Progress)

1495. Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1496. All Bellwether Plaintiffs bring this claim against Progress on behalf of the Progress Nationwide Class or, in the alternative, the Progress State Classes.

1497. M.G.L. ch. 93A § 2 provides that "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."

M.G.L. ch. 93A § 9 permits any consumer injured by a violation of M.G.L. ch. 93A § 2 to bring a civil action, including a class action, for damages and injunctive relief.

1498. Plaintiffs allege Progress committed unfair business acts and/or practices in violation of M.G.L. ch. 93A §§ 2 and 9.

1499. Progress knew or should have known of the inherent risks in experiencing a data breach if it failed to maintain adequate systems and processes for keeping Plaintiffs' and Progress Bellwether Class Members' Private Information safe and secure. Only Progress was in a position to ensure that its systems were sufficient to protect against harms to Plaintiffs and the Progress Bellwether Class Members resulting from a data security incident such as the Data Breach; instead, it failed to implement such safeguards.

1500. Progress's own conduct also created a foreseeable risk of harm to Plaintiffs and Progress Bellwether Class Members and their Private Information. Progress's misconduct included failing to adopt, implement, and maintain the systems, policies, and procedures necessary to prevent the Data Breach.

1501. Progress acknowledges its conduct created actual harm to Plaintiffs and Progress Bellwether Class Members because Progress instructed them to monitor their accounts for fraudulent conduct and identity theft.

1502. Progress knew, or should have known, of the risks inherent in disclosing, collecting, storing, accessing, and transmitting Private Information and the importance of adequate security because of, *inter alia*, the prevalence of data breaches.

1503. Progress failed to adopt, implement, and maintain fair, reasonable, or adequate security measures to safeguard Plaintiffs' and Progress Bellwether Class Members' Private Information, failed to recognize in a timely manner the Data Breach, and failed to notify Plaintiffs

and Progress Bellwether Class Members in a timely manner that their Private Information was accessed in the Data Breach.

1504. These acts and practices are unfair in material respects, offend public policy, are immoral, unethical, oppressive and unscrupulous and violate 201 CMR 17.00 and M.G.L. ch. 93A § 2.

1505. As a direct and proximate result of Progress's unfair acts and practices, Plaintiffs and Progress Bellwether Class Members have suffered injury and/or will suffer injury and damages, including, but not limited to: (i) the loss of the opportunity to determine for themselves how their Private Information is used; (ii) the publication and/or fraudulent use of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of Progress's Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest and recover from unemployment and/or tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Private Information, which remains in Progress's possession (and/or to which Progress continues to have access) and is subject to further unauthorized disclosures so long as Progress fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of disclosed Private Information.

1506. Neither Plaintiffs nor the other Progress Bellwether Class Members contributed to Progress's Data Breach.

1507. Plaintiffs sent a demand for relief, in writing, to Progress on June 4, 2024, prior to filing this complaint. Multiple Plaintiffs in consolidated actions have sent[451]—or alleged in their complaints that they would send[452]—similar demand letters as required by M.G.L. c. 93A § 9. Plaintiffs have not received a written tender of settlement that is reasonable in relation to the injury actually suffered by Plaintiffs and the Progress Bellwether Class Members.

1508. Based on the foregoing, Plaintiffs and the other Members of the Progress Bellwether Class are entitled to all remedies available pursuant to M.G.L ch. 93A, including, but not limited to, refunds, actual damages, or statutory damages in the amount of twenty-five dollars per violation, whichever is greater, double or treble damages, attorneys' fees and other reasonable costs.

---

[451] *See, e.g.*, *Ghalem, et al. v. Progress Software Corp., et al.*, 23-cv-12300 (D. Mass.), at ECF No. 1, ¶ 213 ("A demand identifying the claimant and reasonably describing the unfair or deceptive act or practice relied upon and the injury suffered was mailed or delivered to Defendants at least thirty days prior to the filing of a pleading alleging this claim for relief").

[452] In all of the following cases (among others), plaintiffs indicated that they were going to send similar demand letters: *Allen, et al. v. Progress Software Corp*., 23-cv-11984 (D. Mass.); *Anastasio v. Progress Software Corp., et al*., 23-cv-11442 (D. Mass.); *Arden v. Progress Software Corp., et al*., 23-cv-12015 (D. Mass.); *Boaden v. Progress Software Corp., et al*., 23-cv-12192 (D. Mass.); *Brida v. Progress Software Corp., et al*., 23-cv-12202 (D. Mass.); *Casey v. Progress Software Corp., et al*., 23-cv-11864 (D. Mass.); *Constantine v. Progress Software Corp., et al*., 23-cv-12836 (D. Mass.); *Daniels v. Progress Software Corp., et al*., 23-cv-12010 (D. Mass.); *Doe v. Progress Software Corp., et al*., 23-cv-1933 (D. Md.); *Ghalem, et al. v. Progress Software Corp., et al*., 23-cv-12300 (D. Mass.); *Kennedy v. Progress Software Corp., et al*., 23-cv-12275 (D. Mass.); *Kurtz v. Progress Software Corp., et al*., 23-cv-12156 (D. Mass.); *McDaniel, et al. v. Progress Software Corp., et al*., 23-cv-11939 (D. Mass.); *Pilotti-Iulo v. Progress Software Corp., et al*., 23-cv-12157 (D. Mass.); *Pulignani v. Progress Software Corp., et al*. , 23-cv-1912 (D. Md.); *Siflinger, et al. v. Progress Software Corp., et al*., 23-cv-11782 (D. Mass.); *Tenner v. Progress Software Corp*., 23-cv-11412 (D. Mass.); *Truesdale v. Progress Software Corp., et al*., 23-cv-1913 (D. Md.).

1509. Pursuant to M.G.L. ch. 231, § 6B, Plaintiffs and other Members of the Progress Bellwether Class are further entitled to pre-judgment interest as a direct and proximate result of Progress's wrongful conduct. The amount of damages suffered as a result is a sum certain and capable of calculation, and Plaintiffs and Progress Bellwether Class Members are entitled to interest in an amount according to proof.

PROGRESS BELLWETHER NINTH CLAIM FOR RELIEF
California Consumer Privacy Act
Cal. Civ. Code §§ 1798.100 *et seq*., § 1798.150(a)
(Brought by Plaintiffs Camille Burgan, Eugene Burgan, Amanda Copans, Deanna Duarte, Brinitha Harris, Shellie McCaskell, Denise Meyer, Ricardo Moralez, and Rita Pasquarelli on behalf of the Progress California Class against Progress)

1510. Plaintiffs C. Burgan, E. Burgan, Copans, Duarte, Harris, McCaskell, Meyer, Moralez, and Pasquarelli (collectively, the "California Progress Plaintiffs") reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1511. The California Progress Plaintiffs bring this claim against Progress on behalf of the Progress California Class (the "California Class").

1512. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

1513. Progress is a "business" in that it is a corporation that is organized or operated for the profit or financial benefit of its shareholders or other owners, with annual gross revenues over $25 million.

1514. The Progress California Plaintiffs and California Class Members are "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

1515. The Private Information of the Progress California Plaintiffs and California Class Members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the personal information Progress's clients collected and stored (using Progress' MOVEit software) that was impacted by the Data Breach included an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; and (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

1516. Progress marketed, sold, and assumed responsibility for the continuing maintenance and security of its MOVEit software, with the intent and knowledge that the customers of Progress's clients (including the Progress California Plaintiffs and the California

Class Members) would depend on Progress's MOVEit software to securely store and transfer their Private Information.

1517. Progress knew or should have known that its MOVEit computer system software and data security practices were inadequate to safeguard the Progress California Plaintiffs' and California Class Members' Private Information and that the risk of a data breach or theft was highly likely. Progress failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the Private Information of the Progress California Plaintiffs and the California Class Members.

1518. Progress's failure to implement proper security procedures and practices allowed for CL0P to access, decrypt, and exfiltrate the Progress California Plaintiffs' and California Subclass Members' "nonencrypted and unredacted personal information" as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d), in the Data Breach.

1519. As a direct and proximate result of Progress's violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of the Progress California Plaintiffs' and California Class Members' Private Information included exfiltration, theft, or disclosure by and/or to hacker who further disclosed the Private Information alleged herein on the dark web.

1520. As a direct and proximate result of Progress's acts, the Progress California Plaintiffs and California Class Members were injured and lost money or property, including, but not limited to, the loss of the Progress California Plaintiffs' and California Class Members' legally protected interest in the confidentiality and privacy of their Private Information, stress, fear, and anxiety, nominal damages, and additional losses described above.

1521. The Progress California Plaintiffs have complied with the requirements of California Civil Code Section 1798.150(b), which provides that "[n]o [prefiling] notice shall be

required prior to an individual consumer initiating an action solely for actual pecuniary damages." On June 11 and June 12, 2024, Plaintiff Copans and Plaintiff Meyer, respectively, provided Progress with written notice identifying Progress's violations of Cal. Civil Code § 1798.150(a) and demanding the Data Breach be cured, pursuant to Cal. Civil Code § 1798.150(b). Within 30 days of receiving Plaintiffs' notices, Progress neither cured the noticed violations nor provided Plaintiffs Copans and Meyer with an express written statement that the violations have been cured and that no further violations shall occur.

1522. Because Progress has neither cured the noticed violation nor provided the Progress California Plaintiffs with an express written statement that the violations have been cured and that no further violations shall occur:

a. The Progress California Plaintiffs seek injunctive relief in the form of an order requiring Progress to employ adequate security practices consistent with law and industry standards to protect the California Class Members' Private Information; and

b. The Progress California Plaintiffs and the California Class Members seek statutory damages or actual damages, whichever is greater, pursuant to Cal. Civil Code § 1798.150(a)(1)(A) & (B).

PROGRESS BELLWETHER TENTH CLAIM FOR RELIEF
California Consumer Legal Remedies Act
Cal. Civ. Code §§ 1750, *et seq*.
(Brought by Plaintiffs Camille Burgan, Eugene Burgan, Amanda Copans, Deanna Duarte, Brinitha Harris, Shellie McCaskell, Denise Meyer, and Ricardo Moralez, and Rita Pasquarelli on behalf of the Progress Nationwide Class, or, in the alternative, the Progress California Class, against Progress)

1523. The California Progress Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1524. The California Progress Plaintiffs bring this claim against Progress on behalf of the Progress Nationwide Class, or in the alternative, the Progress California Class.

1525. At all relevant times, the Progress California Plaintiffs and California Class Members were "consumers" as under the terms of the CLRA as individuals seeking or acquiring, by purchase or lease, goods or services for personal, family, or household purposes.

1526. At all relevant times Progress's actions and conduct resulted in transactions for the sale or lease of goods or services to consumers under the terms of the Consumer Legal Remedies Act ("CLRA"). Specifically, the goods and services offered and sold by the companies who purchased and relied on Progress's MOVEit software to handle their customers' Private Information constitute "services" under the CLRA.

1527. By the acts described above, Progress violated California Civil Code section 1770(a)(5), by the use of untrue or misleading statements and omissions and representing that its MOVEit software had characteristics or benefits that it knew to be untrue.

1528. By the acts described above, Progress violated California Civil Code section 1770(a)(14), by representing to its clients and the public at large that its MOVEit software employed the highest level of data security and would protect and safeguard Private Information from unauthorized, knowing and intending that its clients would pass these representations along to the Progress California Plaintiffs and California Class Members, when in fact Progress knew such benefits were not conferred.

1529. Progress knew, or should have known, that its representations and advertisements about the nature of its data security and its promise to maintain and update the ability of its MOVEit software to securely store and transfer Private Information were false or misleading and were likely to deceive a reasonable consumer. No reasonable consumer would use Progress's services if they knew that Progress was not taking reasonable measures to safeguard their Private Information.

1530. As a direct and proximate result of Progress's violations of California Civil Code § 1770, the Progress California Plaintiffs and California Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information, including, but not limited to, the diminishment of their present and future property interest in their Private Information and the deprivation of the exclusive use of their Private Information.

1531. Pursuant to California Civil Code § 1782(d), the Progress California Plaintiffs provided notice of their claims for damages on November 11, 2024.

1532. Within 30 days of receiving the Progress California Plaintiffs' notices, Progress did not cure the noticed violations of the CLRA, nor did it provide Progress California Plaintiffs with an express written statement that the violations have been cured and that no further violations shall occur.

1533. The Progress California Plaintiffs and California Class Members seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

PROGRESS BELLWETHER ELEVENTH CLAIM FOR RELIEF
California Confidentiality of Medical Information Act ("CMIA")
Cal. Civ. Code §§ 56, *et seq.*
(Brought by Plaintiffs Amanda Copans, Deanna Duarte, Shellie McCaskell, Denise Meyer, and Ricardo Moralez on behalf of the Progress California PHI Class, against Progress)

1534. Plaintiffs Copans, Deanna Duarte, Shellie McCaskell, Denise Meyer, and Ricardo Moralez (collectively, the "Progress California PHI Plaintiffs") reallege and incorporate by

reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two..

1535. Progress California PHI Plaintiffs bring this claim against Progress on behalf of the Progress California Class.

1536. The California's Confidentiality of Medical Information Act ("CMIA") prohibits, among other things, unauthorized disclosure of private medical information. Cal. Civ. Code §§ 56, et seq.

1537. The Progress California PHI Plaintiffs and Progress California PHI Class Members provided their Private Information to clients of Progress who qualify as "Provider[s] of health care," as defined by Cal. Civ. Code § 56.05(j) who, in turn, used Progress's MOVEit software in order to provide healthcare services.

1538. The Progress California PHI Plaintiffs and Progress California PHI Class Members are "patients," as defined by Cal. Civ. Code § 56.05(m).

1539. Progress is subject to the CMIA, in accordance with California Civil Code § 56.06(b), to the extent that it is a "business that offers software . . . to consumers, . . . that is designed to maintain medical information in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage the individual's information."

1540. At all relevant times, Progress's clients relied on Progress's MOVEit software to collect, store, manage and/or transmit the Progress California PHI Plaintiffs' and Progress California PHI Class Members' Private Information including, but not limited to, "medical information" as defined by Cal. Civ. Code § 56.05(j).

1541. Progress's MOVEit software was designed, in part, to make medical information available to health care providers and other similar entities so that those organizations could store, access, and manage consumers' medical information, in order to provide services that include diagnosing, treating, or managing consumers' medical conditions.

1542. The Progress California PHI Plaintiffs and Progress California PHI Class Members did not provide Progress and/or its direct or indirect clients with authorization, nor were Progress and/or its direct or indirect clients authorized, to disclose the Progress California PHI Plaintiffs' and Progress California PHI Class Members' medical information to an unauthorized third-party.

1543. As described throughout this Complaint, Progress negligently maintained its MOVEit software, and, as a proximate and foreseeable result, Progress California PHI Plaintiffs' and Progress California PHI Class Members' medical information that had been entrusted to the MOVEit software was disclosed and released. Specifically, Progress and its clients did not implement adequate security protocols to prevent unauthorized access to medical information, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially viable measures to mitigate the risks of any data the risks of any data breach or otherwise comply with HIPAA data security requirements.

1544. Progress's conduct constitutes a violation of Sections 56.06 and 56.101 of the California CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential personal medical information.

1545. As a direct and proximate result of Progress's negligence, the Progress California PHI Plaintiffs' and Progress California PHI Class Members' medical information was disclosed and/or released to an unauthorized third-party.

1546. Progress's negligence, causing the unauthorized disclosure of medical records, has, in turn, caused injury to the Progress California PHI Plaintiffs and the Progress California PHI Class Members.

1547. Upon information and belief, the Progress California PHI Plaintiffs' and the Progress California PHI Class Members' confidential medical information has been viewed by an unauthorized third party.

1548. As a direct and proximate result of Progress's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and Progress' violations of the CMIA, the Progress California PHI Plaintiffs and Progress California PHI Class Members are entitled to (i) actual damages, (ii) nominal damages of $1,000 per Plaintiff and Class Member, and (iii) attorneys' fees, litigation expenses and court costs under California Civil Code § 56.35.

PROGRESS BELLWETHER TWELFTH CLAIM FOR RELIEF
California Customer Records Act
Cal. Civ. Code § 1798.80, *et seq*.
(Brought by Plaintiffs Camille Burgan, Eugene Burgan, Amanda Copans, Deanna Duarte, Brinitha Harris, Shellie McCaskell, Denise Meyer, Ricardo Moralez, and Rita Pasquarelli on behalf of the Progress Nationwide Class, or, in the alternative, the Progress California Class, against Progress)

1549. The California Progress Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1550. The California Progress Plaintiffs bring this claim against Progress on behalf of the Progress Nationwide Class, or in the alternative, the Progress California Class.

1551. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that Private Information about California residents is protected. To that end, the purpose of

this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

1552. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

1553. Cal. Civ. Code § 1798.84(b) provides that "[a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

1554. The Progress California Plaintiffs and California Class Members are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to Progress's direct or indirect customers using MOVEit software to protect, encrypt, and transfer Private Information for the purpose of obtaining healthcare services from Progress's clients.

1555. Progress's direct or indirect customers purchased and employed Progress's MOVEit software in furtherance of their business operations, which includes owning, maintaining, and licensing the Progress California Plaintiffs' and California Class Members' "personal information" within the meaning of Cal. Civ. Code § 1798.81.5(d)(1)). Additionally, Progress uses its own MOVEit software service to engage in business operations that involve owning, maintaining, and licensing "personal information" within the meaning of Cal. Civ. Code § 1798.81.5(d)(1).

1556. The Private Information of the Progress California Plaintiffs and California Class Members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and

1798.81.5, in that the personal information Progress's clients collected and stored (using Progress's MOVEit software) that was impacted by the Data Breach included an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; and/or (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

1557. Moreover, Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay . . . ."

1558. Any person or business that is required to issue a security breach notification under the CCRA must meet the following requirements under § 1798.82(d):

a. The name and contact information of the reporting person or business subject to this section;

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

i. the date of the breach,

ii. the estimated date of the breach, or

iii. the date range within which the breach occurred. The notification shall also include the date of the notice.

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

1559. Progress provides data interoperability solutions to its clients. Progress provides services wherein its direct or indirect clients provide it with computerized data that includes personal information that Progress owns, maintains and/or licenses. In addition, Progress manufactures, maintains, and sells its MOVEit software to clients with the knowledge that, and for the purpose of, its clients will use Progress's MOVEit software to facilitate the ownership, licensing and/or sale of computerized data that includes personal information as defined by Cal Civ. Code § 1798.82(h).

1560. The Progress California Plaintiffs' and California Class Members' Private Information includes "personal information" as covered by Cal. Civ. Code §§ 1798.81.5(d)(1), 1798.82(h).

1561. The Data Breach described herein constituted a "breach of the security system" to the extent that the hackers breached Progress' MOVEit software.

1562. Because Progress reasonably believed that the Progress California Plaintiffs' and California Class Members' Private Information was acquired by unauthorized persons during the Data Breach as a result of the MOVEit software's security vulnerabilities, Progress had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

1563. As alleged above, Progress unreasonably delayed informing the Progress California Plaintiffs and California Class Members about the Data Breach, affecting their Private Information, after Progress knew when and how the Data Breach had occurred.

1564. By failing to disclose the Data Breach in a timely and accurate manner, Progress violated Cal. Civ. Code § 1798.82.

1565. As a result of Progress's violation of Cal. Civ. Code § 1798.82, the Progress California Plaintiffs and California Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by the Progress California Plaintiffs and California Class Members because their stolen information would have had less value to identity thieves.

1566. As a result of Progress's violation of Cal. Civ. Code § 1798.82, the Progress California Plaintiffs and California Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

1567. As a direct consequence of the actions as identified above, Progress California Plaintiffs and California Class Members incurred additional losses and suffered further harm to

their privacy, including, but not limited to, economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

PROGRESS BELLWETHER THIRTEENTH CLAIM FOR RELIEF
California Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, et seq.
(Brought by Plaintiffs Camille Burgan, Eugene Burgan, Amanda Copans, Deanna Duarte, Brinitha Harris, Shellie McCaskell, Denise Meyer, Ricardo Moralez, and Rita Pasquarelli on behalf of the Progress Nationwide Class, or, in the alternative, the Progress California Class, against Progress)

1568. The California Progress Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1569. The California Progress Plaintiffs bring this claim against Progress on behalf of the Progress Nationwide Class, or in the alternative, the Progress California Class.

1570. Progress is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

1571. Progress violated Cal. Bus. & Prof. Code §§ 17200, *et seq*. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

1572. Progress's "unfair" acts and "deceptive" practices include:

a. Progress failed to maintain and update its MOVEit software, including failing to implement reasonable security measures that would have protected the Progress California Plaintiffs' and California Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Progress failed to identify foreseeable security risks, remediate identified

security risks, and adequately improve security following previous cybersecurity incidents involving its MOVEit software.

b. Progress's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), HIPAA, 42 U.S.C. § 1320d, California's Consumer Records Act (Cal. Civ. Code § 1798.81.5), California's Consumer Legal Remedies Act (Cal Civ. Code § 1780, et seq.), and the Confidentiality of Medical Information Act (Cal Civ. Code § 56.26(b)).

c. Progress's failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Progress' inadequate security, consumers could not have reasonably avoided the harms that Progress caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

1573. Progress has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, et. seq. (requiring reasonable data security measures), California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTC Act, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d.

1574. Progress's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect the Progress California Plaintiffs' and California Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of the Progress California Plaintiffs' and California Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of the Progress California Plaintiffs' and California Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that its MOVEit software complied with common law and statutory duties pertaining to the security and privacy of the Progress California Plaintiffs' and California Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.;

f. Failing to timely and adequately notify the Progress California Plaintiffs and California Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that its MOVEit software did not reasonably or adequately secure the Progress California Plaintiffs' and California Class Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that its MOVEit software did not comply with common law and statutory duties pertaining to the security and privacy of the Progress California Plaintiffs' and California Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d., and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*.

1575. Progress's representations and omissions regarding its MOVEit software were material because they were likely to deceive reasonable consumers about the adequacy of its direct and indirect customers' data security and the ability of its MOVEit software to protect the confidentiality of consumers' Private Information.

1576. As a direct and proximate result of Progress's unfair, unlawful, and fraudulent acts and practices, the Progress California Plaintiffs and California Class Members were injured and lost money or property, including the costs passed through Progress and/or its clients, the

premiums and/or prices paid to Progress clients for their goods and services, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Private Information.

1577. Progress acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded the Progress California Plaintiffs' and California Class Members' rights. Past file transfer data breaches as well as other data breaches in the healthcare industry put Progress on notice that its security and privacy protections were inadequate.

1578. Unless restrained and enjoined, Progress will continue to engage in the above-described wrongful conduct and more data breaches will occur.

1579. As such, the Progress California Plaintiffs on behalf of themselves and California Class Members, seek restitution and an injunction, including public injunctive relief prohibiting Progress from continuing such wrongful conduct, and requiring Progress to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect Private Information entrusted to its MOVEit software, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

1580. To the extent any of these remedies are equitable, the Progress California Plaintiffs and the California Class Members seek such equitable remedies, in the alternative to any adequate remedy at law they may have, including under California's Consumer Privacy Act, California's Consumers Legal Remedies Act, California's Confidentiality of Medical Information Act, California's Customer Records Acts, California's Constitution, HIPAA, and HITECH.

PROGRESS BELLWETHER FOURTEENTH CLAIM FOR RELIEF
California Constitution's Right to Privacy
Cal. Const., Art. I, § I
(Brought by Plaintiffs Camille Burgan, Eugene Burgan, Amanda Copans, Deanna Duarte, Brinitha Harris, Shellie McCaskell, Denise Meyer, Ricardo Moralez, and Rita Pasquarelli, on behalf of the Progress Nationwide Class, or, in the alternative, the Progress California Class, against Progress)

1581. The California Progress Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1582. The California Progress Plaintiffs bring this claim against Progress on behalf of the Progress Nationwide Class, or in the alternative, the Progress California Class.

1583. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

1584. The right to privacy in California's Constitution creates a private right of action against private and government entities.

1585. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

1586. Progress violated the Progress California Plaintiffs' and California Class Members' constitutional right to privacy by facilitating the collection and storage of their Private Information and by then disclosing, or preventing from unauthorized disclosure, their Private Information, which includes information in which they had a legally protected privacy interest, and for which

they had a reasonable expectation of privacy. Disclosure of their Private Information was highly offensive given the highly sensitive nature of the data. Disclosure of their private medical information in particular could cause humiliation to the Progress California Plaintiffs and California Class Members. Accordingly, disclosure of the Progress California Plaintiffs' and California Class Members' Private Information is an egregious violation of social norms.

1587. Progress intruded upon the Progress California Plaintiffs' and California Class Members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential Private Information.

1588. The Progress California Plaintiffs and California Class Members had a reasonable expectation of privacy in that: (i) their invasion of privacy occurred as a result of Progress's lax and inadequate security practices with respect to securely developing and maintaining its MOVEit software, which facilitated the collection, storage, and use of Progress California Plaintiffs' and California Class Members' data, as well as with respect to preventing the unauthorized disclosure of their Private Information; (ii) the Progress California Plaintiffs and California Class Members did not consent or otherwise authorize Progress to disclose their Private Information to parties responsible for the cyberattack; and (iii) the Progress California Plaintiffs and California Class Members could not reasonably expect Progress would commit acts in violation of laws protecting their privacy.

1589. As a result of Progress's actions, the Progress California Plaintiffs and California Class Members have been damaged as a direct and proximate result of Progress's invasion of their privacy and are entitled to just compensation.

1590. The Progress California Plaintiffs and California Class Members suffered actual and concrete injury as a result of Progress's violations of their privacy interests. The Progress

California Plaintiffs and California Class Members are entitled to appropriate relief, including damages to compensate them for the harms to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Progress's invasions.

1591. The Progress California Plaintiffs and California Class Members seek appropriate relief for that injury, including, but not limited to, damages that will reasonably compensate them for the harm to their privacy interests as well as disgorgement of profits made by Progress as a result of their intrusions upon the Progress California Plaintiffs' and California Class Members' privacy.

PROGRESS BELLWETHER FIFTEENTH CLAIM FOR RELIEF
Connecticut Unfair Trade Practices Act ("CUTPA")
Conn. Gen. Stat. § 42-110B
(Brought by Karen Boginski on behalf of the Progress Connecticut Class)

1592. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1593. Plaintiff Karen Boginski brings this claim against Progress on behalf of the Progress Connecticut Class (the "Connecticut Class").

1594. Progress, Plaintiff Boginski, and Connecticut Class Members are "persons" within the meaning of Conn. Gen. Stat. § 42- 110a(3).

1595. The Connecticut Unfair Trade Practices Act ("CUTPA") provides: "No person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." Conn. Gen. Stat. § 42-110b(a).

1596. Progress advertised, offered, sold, or distributed "property" in Connecticut and engaged in trade or commerce directly or indirectly affecting persons in Connecticut. Conn. Gen. Stat. § 42-110a(4).

1597. CUTPA provides that "[a]ny person who suffers an ascertainable loss of money or property, real or personal, as a result of the use or employment of a method, act or practice prohibited by section 42-110b, may bring an action . . . to recover actual damages." Conn. Gen. Stat. § 42-110g(a).

1598. Plaintiff Boginski and Connecticut Class Members have a private right of action under Conn. Gen. Stat. § 42-110g(a).

1599. Progress engaged in unfair or deceptive acts or practices in violation of Conn. Gen. Stat. § 42-110b(a) by, among other things:

a. Failing to implement and maintain reasonable security measures to protect Plaintiff Boginski's and Connecticut Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach, Plaintiff Boginski's and Connecticut Class Members' Private Information being compromised, and subsequent harms caused to Plaintiff Boginski and the Connecticut Class;

b. Failing to identify foreseeable security risks, remediate identified security risks, and sufficiently improve security following previous cybersecurity incidents, as alleged herein. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff Boginski and Connecticut Class Members, whose Private Information has been compromised;

c. Misrepresenting, omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections it had in place to protect the Private Information of Plaintiff Boginski and the Connecticut Class.

1600. Progress's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45. Similarly, policies of the importance of protecting individuals' PHI are reflected in HIPAA, 45 C.F.R. § 164; HITECH Act, 42 U.S.C. § 17902; and Conn. Gen. Stat. § 36A-701B.

1601. CUTPA provides that in its interpretation and application, the courts "shall be guided by interpretations given by the Federal Trade Commission and the federal courts to Section 5(a)(1) of the Federal Trade Commission Act (15 USC 45(a)(1)), as from time to time amended." Conn. Gen. Stat. § 42-110b(b). As discussed, supra, the FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

1602. Progress's failure to adequately safeguard Plaintiff Boginski and Connecticut Class Members' Private Information, constituting an unfair act under Gen. Stat. § 42-110b, was immoral, unethical, oppressive, and unscrupulous.

1603. Progress was aware that the healthcare industry was a frequent target of sophisticated cyberattacks. Progress knew or should have known that its data security was insufficient to guard against those attacks, particularly, given its direct or indirect clients who used its MOVEit software to collect, store, and transfer sensitive Private Information therein.

1604. Progress knew or should have known that its data security practices were deficient, inadequate, and did not satisfy industry or regulatory standards for the purposes of protecting consumers' Private Information. Progress knew or should have known that its data security was insufficient to guard against those attacks, particularly, given its direct or indirect clients' use of its MOVEit software to collect, store, and transfer sensitive Private Information therein.

1605. Progress should have taken adequate measures to protect the data that its direct or indirect customers collected, transferred, or stored on its MOVEit software. Progress's above-described conduct was negligent, knowing and willful, and/or wanton and reckless.

1606. Progress's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of their data security policies and

practices and ability to protect the confidentiality of consumers' Private Information and thus were immoral, unethical, oppressive, and unscrupulous.

1607. Progress's acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

1608. As a direct and proximate result of Progress's deceptive acts and practices, Plaintiff Boginski and the Connecticut Class Members suffered ascertainable losses, including the loss of their legally protected interest in the confidentiality and privacy of their Private Information, diminution in value of their Private Information, loss of time and opportunity costs, among others alleged herein.

1609. Additionally, as alleged, infra, Progress's actions in violation of the CUTPA include, but are not limited to its failure to disclose the Data Breach in a timely and accurate manner as required by C.G.S.A. § 36a-701b(b) and (c).

1610. Progress's failure to disclose the Data Breach in a timely and accurate manner was misleading to Plaintiff Boginski and the Connecticut Class Members as they reasonably believed their Private Information and other private and confidential information was secured by Progress due to the sensitive nature of the data and special relationship they held, and promises of data security and privacy contained in multiple privacy policies and documents, among other reasons.

1611. Progress's failure to disclose was material since it affected Plaintiff Boginski and Connecticut Class Members' decisions, including, but not limited to:

a. whether to continue to provide Private Information or other private and confidential information to companies that utilized MOVEit software;

b. whether to pay for services to attempt to secure Private Information compromised by the Data Breach;

c. whether to seek the advice of counsel and/or seek legal representation; and

d. whether to continue to use the services of companies that utilized MOVEit software.

1612. Progress's failure to disclose in a timely and accurate manner was immoral, unethical, oppressive, or unscrupulous since it deprived Plaintiff Boginski and Connecticut Class Members of important knowledge about their compromised Private Information and delayed any ability they had to try and secure their Private Information and other private and confidential information.

1613. Furthermore, Progress's failure to disclose in a timely and accurate manner has caused substantial injury to Plaintiff Boginski and Connecticut Class Members since they were deprived of the knowledge their Private Information was compromised, and lost a substantial amount of time in which they could have acted to secure their Private Information in avoidance of the imminent, impending threats of identity theft, fraud, scams; loss of value of their stolen Private Information; illegal sales of the compromised Private Information on the black market; other misuses of their Private Information; monetary loss and economic harm; the need to pay for mitigation expenses and spend time spent monitoring credit; identity theft insurance costs; credit freezes/unfreezes, time spent initiating fraud alerts and contacting third parties; decreased credit scores; lost work time; mental anguish; and other injuries due to the Data Breach.

1614. Progress's failure to disclose the Data Breach in a timely and accurate fashion as described above constitutes an unfair or deceptive act or practice in violation of CUTPA, C.G.S.A. § 42-110b.

1615. As a result of Progress's failure to disclose the Data Breach in a timely and accurate fashion, Plaintiff Boginski and Connecticut Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages including, but not limited to, fraud and identity theft, time and expenses related to monitoring their

financial accounts for fraudulent activity; an increased, imminent and impending threat of fraud and identity theft, loss of value of their Private Information; overpayment for services provided by direct users, vendors, vendor contracting entities, and vendor contracting entity customers who used MOVEit; loss of the value of access to their Private Information; and the value of identity and credit protection and repair services made necessary by the Data Breach.

1616. Plaintiff Boginski and the Connecticut Class Members seek relief under Conn. Gen. Stat. § 42-110g, including actual damages, punitive damages, injunctive relief, and attorneys' fees, expenses, and costs.

PROGRESS BELLWETHER SIXTEENTH CLAIM FOR RELIEF
Georgia Uniform Deceptive Trade Practices Act ("GUDTPA")
Ga. Code Ann. §§ 10-1-370, *et seq.*
(Brought by Doris Cadet and Taneisha Robertson on behalf of the Progress Georgia Class)

1617. Plaintiffs reallege and incorporate by all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1618. Plaintiffs Doris Cadet and Taneisha Robertson bring this claim against Progress on behalf of the Progress Georgia Class (the "Georgia Class").

1619. Progress, Plaintiffs Cadet and Robertson, and Georgia Class Members are "persons" within the meaning of Ga. Code Ann. § 10-1-371(5).

1620. Progress engaged in deceptive trade practices in the conduct of its businesses, in violation of Ga. Code Ann. § 10-1-372(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with the intent not to sell them as advertised;

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

1621. Progress's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs Cadet's and Robertson's and Georgia Class Members' Private Information, which was a direct and proximate cause of the Data Breach, their Private Information being compromised in the Data Breach and subsequent harms;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach, their Private Information being compromised in the Data Breach and subsequent harms;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Cadet's and Robertson's and Georgia Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902, which was a direct and proximate cause of the Data Breach, their Private Information being compromised in the Data Breach and subsequent harms;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs Cadet's and Robertson's and Georgia Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Cadet's and Robertson's and Georgia Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; and HIPAA, 45 C.F.R. § 164;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiffs Cadet's and Robertson's and Georgia Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Cadet's and Robertson's and Georgia Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902.

1622. Progress's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security policies and practices and ability to protect the confidentiality of consumers' Private Information.

1623. In the course of its business, Progress engaged in activities with a tendency or capacity to deceive.

1624. Progress acted intentionally, knowingly, and maliciously to violate Georgia's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs Cadet's and Robertson's and Georgia Class Members' rights.

1625. Had Progress disclosed to consumers that it was not complying with industry standards or regulations or that their data systems were not secure and, thus, was vulnerable to attack, it would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

1626. Instead, Progress was entrusted, either directly or indirectly, with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs Cadet and Robertson and Georgia Class Members. Progress accepted the critical responsibility of protecting the data but kept the inadequate state of their security controls secret from the public. Accordingly, Plaintiffs Cadet and Robertson and Georgia Class Members acted reasonably in relying on Progress's misrepresentations and omissions, the truth of which they could not have discovered.

1627. As a direct and proximate result of Progress's unfair, unlawful, and fraudulent acts and practices, Plaintiffs Cadet and Robertson and Georgia Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including, but not limited to, fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for services provided by users of MOVEit software; loss of the value of access to their Private Information; diminution of value of Private Information; value of identity and credit protection

and repair services made necessary by the Data Breach; and they face ongoing risks of future harms insofar as has have yet to implement the necessary policies, practices, and measures to adequately safeguard their Private Information in compliance with laws and industry standards.

1628. Plaintiffs Cadet and Robertson and Georgia Class Members seek all relief allowed by law, including injunctive relief, which is necessary to prospectively protect against future data breaches, and reasonable attorneys' fees and costs, under Ga. Code Ann. § 10-1-373.

PROGRESS BELLWETHER SEVENTEENTH CLAIM FOR RELIEF
Illinois Private Information Protection Act
815 Ill. Comp. Stat. §§ 530/10(a), *et seq*.
(Brought by Rob Plotke, Christopher Rehm, and Katharine Uhrich on behalf of the Progress Illinois Classes)

1629. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1630. Plaintiffs Rob Plotke, Christopher Rehm, and Katharine Uhrich (collectively, the "Progress Illinois Plaintiffs") bring this claim against Progress on behalf of the Progress Illinois Class (the "Illinois Class").

1631. Progress, as an entity that facilitates and/or takes responsibility for the collection, handling, dissemination, and other dealings with nonpublic Private Information, Progress qualifies as a Data Collector, as defined in 815 Ill. Comp. Stat. § 530/5.

1632. Progress Illinois Plaintiffs' and Illinois Class Members' Private Information (e.g., Social Security numbers) includes Private Information as covered under 815 Ill. Comp. Stat. § 530/5.

1633. As a Data Collector, Progress is required to notify the Progress Illinois Plaintiffs and Illinois Class Members of a breach of its MOVEit data security system in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. § 530/10(a).

1634. The Data Breach described herein constituted a "breach of the [Progress MOVEit] security system."

1635. Because Progress knew or reasonably believed that Progress Illinois Plaintiffs' and Illinois Class Members' Private Information was acquired by unauthorized persons during the Data Breach, Progress had an obligation to disclose the Data Breach in a timely and accurate fashion.

1636. As alleged above, Progress unreasonably delayed informing Progress Illinois Plaintiffs and Illinois Class Members about the Data Breach, affecting their Private Information, after Progress knew that the Data Breach had occurred.

1637. By failing to disclose the Data Breach in the most expedient time possible and without unreasonable delay, Progress violated 815 Ill. Comp. Stat. § 530/10(a).

1638. Pursuant to 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

1639. As a result of Progress's violation of 815 Ill. Comp. Stat. § 530/10(a), Progress Illinois Plaintiffs and Illinois Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Progress Illinois Plaintiffs and Illinois Class Members because their stolen information would have had less value to identity thieves.

1640. As a result of Progress's violation of 815 Ill. Comp. Stat. § 530/10(a), Progress Illinois Plaintiffs and Illinois Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

1641. As a direct and proximate result of Progress's violations of 815 Ill. Comp. Stat. § 530/10(a), Progress Illinois Plaintiffs and Illinois Class Members suffered damages, as described above.

1642. Progress Illinois Plaintiffs and Illinois Class Members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because Progress's willful violations of 815 Ill. Comp. Stat. § 530/10(a), including actual damages, equitable relief, costs, and attorneys' fees.

PROGRESS BELLWETHER EIGHTEENTH CLAIM FOR RELIEF
Illinois Consumer Fraud and Deceptive Business Practices Act
815 ILCS 505/1, *et seq*.
(Brought by Rob Plotke, Christopher Rehm, and Katharine Uhrich on behalf of the Progress Nationwide Class, or, in the alternative, the Progress Illinois Class)

1643. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1644. The Progress Illinois Plaintiffs bring this claim against Progress on behalf of the Progress Nationwide Class, or, in the alternative, the Progress Illinois Class.

1645. Progress is a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

1646. The Progress Illinois Plaintiff and Illinois Class Members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

1647. Progress's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

1648. Progress's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Progress Illinois Plaintiffs' and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Progress Illinois Plaintiffs' and Illinois Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Progress Illinois Plaintiffs' and Illinois Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Progress Illinois Plaintiffs' and Illinois Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Failing to timely and adequately notify Progress Illinois Plaintiffs and Illinois Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that its MOVEit software did not reasonably or adequately secure Progress Illinois Plaintiffs' and Illinois Class Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Progress Illinois Plaintiffs' and Illinois Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

1649. Progress's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Progress's MOVEit software's data security

and ability of Progress's MOVEit software to protect the confidentiality of consumers' Private Information.

1650. Progress intended to mislead Progress Illinois Plaintiffs and Illinois Class Members and induce them to rely on its misrepresentations and omissions.

1651. The above unfair and deceptive practices and acts by Progress were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

1652. Progress acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Progress Illinois Plaintiffs' and Illinois Class Members' rights. Past file transfer breaches as well as other healthcare industry breaches put Progress on notice that the security and privacy protections of its MOVEit software were inadequate.

1653. As a direct and proximate result of Progress' unfair, unlawful, and deceptive acts and practices, Progress Illinois Plaintiff and Illinois Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1654. Progress Illinois Plaintiffs and Illinois Class Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

PROGRESS BELLWETHER NINETEENTH CLAIM FOR RELIEF
Illinois Uniform Deceptive Trade Practices Act
815 ILCS 510/2, *et seq.*
(Brought by Rob Plotke, Christopher Rehm, and Katharine Uhrich on behalf of the Progress Illinois Class)

1655. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1656. Progress Illinois Plaintiffs bring this claim against Progress on behalf of the Progress Illinois Class.

1657. Progress is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

1658. Progress engaged in deceptive trade practices in the conduct of their business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

1659. Progress's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Progress Illinois Plaintiffs' and Illinois Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Progress Illinois Plaintiffs' and Illinois Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014,

Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that its MOVEit software would protect the privacy and confidentiality of Progress Illinois Plaintiffs' and Illinois Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Progress Illinois Plaintiffs' and Illinois Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Failing to timely and adequately notify Progress Illinois Plaintiffs and Illinois Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that its MOVEit software did not reasonably or adequately secure Progress Illinois Plaintiffs' and Illinois Class Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Progress Illinois Plaintiffs' and Illinois Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

1660. Progress's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of the data security of its MOVEit software and its ability to protect the confidentiality of consumers' Private Information.

1661. The above unfair and deceptive practices and acts by Progress were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Progress Illinois

Plaintiffs and Illinois Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

1662. As a result of Progress's violations of the Illinois Uniform Deceptive Trade Practices Act, Progress Illinois Plaintiffs and Illinois Class Members suffered damages, as described above, and are likely to suffer harm in the future from the deceptive conduct absent injunctive relief.

1663. As a proximate result of Progress's acts and omissions, Progress Illinois Plaintiffs' and the Illinois Class Members' Private Information were acquired by a third party and is now available for disclosure and redisclosure without authorization. Illinois Class Members have already received notifications from banks, credit card companies, and other credit monitoring services that their Private Information has been discovered on the dark web and can thus be used by third-parties at any time.

1664. Progress Illinois Plaintiffs and Illinois Class Members have no adequate remedy at law for the injuries relating to the fact that Progress's MOVEit software continues to be marketed by Progress and used by Progress's clients to possess their Private Information, despite its inadequate cybersecurity system and policies. A judgment for monetary damages will not end Progress's inability and/or refusal to adequately safeguard the Private Information of Progress Illinois Plaintiffs and the Illinois Class Members.

PROGRESS BELLWETHER TWENTIETH CLAIM FOR RELIEF
Michigan Identity Theft Protection Act
Mich. Comp. Laws Ann. § 445.72, *et seq*.
(Brought by Tamara Williams and Jeff Weaver on behalf of the Progress Michigan Class)

1665. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1666. Plaintiffs Tamara Williams and Jeff Weaver bring this claim against Progress on behalf of the Progress Michigan Class (the "Michigan Class").

1667. As an entity that collects, disseminates, and otherwise deals with nonpublic Private Information, and as an entity that designs, licenses, sells and supports software designed for the collection, dissemination, licensing, and handling of nonpublic Private Information, Progress is a "person or agency that owns or licenses data" of Michigan state residents under Mich. Comp. Laws Ann. § 445.72(1)(a).

1668. Plaintiffs Williams and Weaver and Michigan Class Members' Private Information includes "personal information" as covered under Mich. Comp. Laws Ann. § 445.63(r).

1669. Progress is required to notify Plaintiffs Williams and Weaver and Michigan Class Members of a breach of its MOVEit data security system in the most expedient time possible and without unreasonable delay if a Michigan resident's unencrypted and unredacted Private Information is accessed or acquired by an unauthorized person pursuant to Mich. Comp. Laws Ann. § 445.72(1)(a)&(4).

1670. Upon information and belief, Plaintiffs Williams' and Weaver's and Michigan Class Members' unencrypted and unredacted Private Information was accessed and acquired by CL0P during the Data Breach.

1671. The Data Breach described herein constituted a "breach of the security of [Progress' MOVEit] database."

1672. Because Progress discovered a security breach regarding its MOVEit software and because it had notice of the security breach, Progress had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 45.72(4).

1673. Progress and/or its MOVEit customers unreasonably delayed sending Notice Letters notifying Plaintiffs Williams and Weaver and Michigan Class Members of the Data Breach and the effect it had on their Private Information for more than three months after Progress became aware that the Data Breach had occurred.

1674. By failing to disclose the Data Breach expediently and without unreasonable delay, Progress violated Mich. Comp. Laws Ann. § 445.72(1)(a)&(4).

1675. As a direct and proximate result of Progress's violations of Mich. Comp. Laws Ann § 445.72(1)(a) and (4), Plaintiffs Williams and Weaver and Michigan Class Members suffered the damages from the Data Breach, as described above, along with incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

1676. Plaintiffs Williams and Weaver and Michigan Class Members seek relief under Michigan law pursuant to Mich. Comp. Laws Ann. § 445.72(13) and (15), including any applicable civil fine.

PROGRESS BELLWETHER TWENTY-FIRST CLAIM FOR RELIEF
Michigan Consumer Protection Act
Mich. Comp. Laws Ann. § 445.903, *et seq*.
(Brought by Tamara Williams and Jeff Weaver on behalf of the Progress Michigan Class)

1677. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1678. Plaintiffs Tamara Williams and Jeff Weaver bring this claim against Progress on behalf of the Progress Michigan Class.

1679. Progress is a "person" as defined by Mich. Comp. Laws Ann. § 445.902(1)(d).

1680. Progress offered or sold goods or services in Michigan and engaged in "trade or commerce" directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.902(1)(g).

1681. Progress engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c);

b. Representing that its goods and services are of a particular standard or quality if they are of another in violation of Mich. Comp. Laws Ann. § 445.903(1)(e);

c. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb); and

d. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).

1682. Progress's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs Williams' and Weaver's and Michigan Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Williams' and Weaver's and Michigan Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that its MOVEit software would protect the privacy and confidentiality of Plaintiffs Williams' and Weaver's and Michigan Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Williams' and Weaver's and Michigan Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d;

f. Failing to timely and adequately notify the Plaintiffs Williams and Weaver and Michigan Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that its MOVEit software did not reasonably or adequately secure Plaintiffs Williams' and Weaver's and Michigan Class Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Williams' and Weaver's and Michigan Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d.

1683. Progress intended to mislead Plaintiffs Williams and Weaver and Michigan Class Members and induce them to rely on its misrepresentations and omissions.

1684. Progress acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiffs Williams' and Weaver's and Michigan Class Members' rights.

1685. As a direct and proximate result of Progress's unfair, unconscionable, and deceptive practices, Plaintiffs Williams and Weaver and Michigan Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1686. Plaintiffs Williams and Weaver and Michigan Class Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250, injunctive relief, and any other relief that is just and proper.

PROGRESS BELLWETHER TWENTY-SECOND CLAIM FOR RELIEF
Nebraska Consumer Protection Act
Neb. Rev. Stat. §§ 59-1601, et seq.
(Brought by Laquesha George on behalf of the Progress Nebraska Class)

1687. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1688. Plaintiff Laquesha George brings this claim against Progress on behalf of the Progress Nebraska Class (the "Nebraska Class").

1689. Progress is a "person" as defined by Neb. Rev. Stat. § 59-1601(1).

1690. Progress advertised, offered, or sold goods or services in Nebraska and engaged in trade or commerce directly or indirectly affecting the people of Nebraska, as defined by Neb. Rev. Stat. § 59-1601(2).

1691. Progress engaged in unfair and deceptive acts and practices in conducting trade and commerce, in violation of Neb. Rev. Stat. § 59-1602, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff George's and Nebraska Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff George's and Nebraska Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and the Nebraska Data Protection Act, Neb. Rev. Stat. § 87-808, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that its MOVEit software would protect the privacy and confidentiality of Plaintiff George's and Nebraska Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff George's and Nebraska Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and the Nebraska Data Protection Act, Neb. Rev. Stat. § 87-808;

f. Failing to timely and adequately notify the Plaintiff George and Nebraska Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that its MOVEit software did not reasonably or adequately secure Plaintiff George's and Nebraska Class Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff George's and Nebraska Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and the Nebraska Data Protection Act, Neb. Rev. Stat. § 87-808.

1692. Progress's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Progress's MOVEit software's data security and its ability to protect the confidentiality of consumers' Private Information.

1693. As a direct and proximate result of Progress's unfair and deceptive acts and practices, Plaintiff George and Nebraska Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1694. Progress's unfair and deceptive acts and practices complained of herein affected the public interest, including the large number of Nebraskans affected by the Data Breach.

1695. Plaintiff George and Nebraska Class Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, the greater of either (1) actual damages or (2) $1,000, civil penalties, and reasonable attorneys' fees and costs.

PROGRESS BELLWETHER TWENTY-THIRD CLAIM FOR RELIEF
Nebraska Uniform Deceptive Trade Practices Act
Neb. Rev. Stat. §§ 87-301, *et seq*.
(Brought by Laquesha George on behalf of the Progress Nebraska Class)

1696. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1697. Plaintiff Laquesha George brings this claim against Progress on behalf of the Progress Nebraska Class.

1698. Progress is a "person" as defined by Neb. Rev. Stat. § 87-301(19).

1699. Progress advertised, offered, or sold goods or services in Nebraska and engaged in trade or commerce directly or indirectly affecting the people of Nebraska.

1700. Progress engaged in unfair and deceptive acts and practices in conducting trade and commerce, in violation of Neb. Rev. Stat. §§ 87-302(a)(5), (8), and (10), including:

a. Representing that goods and services have characteristics, uses, benefits, or qualities that they do not have;

b. Representing that goods and services are of a particular standard, quality, or grade if they are of another; and

c. Advertising its goods and services with intent not to sell them as advertised and in a manner calculated or tending to mislead or deceive.

1701. Progress's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff George's and Nebraska Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff George's and Nebraska Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and the Nebraska Data Protection Act, Neb.

Rev. Stat. § 87-808, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that its MOVEit software would protect the privacy and confidentiality of Plaintiff George's and Nebraska Class Members' Private Information, including by Progress implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff George's and Nebraska Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and the Nebraska Data Protection Act, Neb. Rev. Stat. § 87-808;

f. Failing to timely and adequately notify the Plaintiff George and Nebraska Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that its MOVEit software did not reasonably or adequately secure Plaintiff George's and Nebraska Class Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff George and Nebraska Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and the Nebraska Data Protection Act, Neb. Rev. Stat. § 87-808.

1702. Progress's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Progress's MOVEit software's data security and its ability to protect the confidentiality of consumers' Private Information.

1703. Progress intended to mislead Plaintiff George and Nebraska Class Members and induce them to rely on its misrepresentations and omissions.

1704. Had Progress disclosed to Plaintiff George and Nebraska Class Members that its MOVEit software was not secure and, thus, vulnerable to attack, Progress would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Progress marketed and sold its MOVEit software knowing that Progress's direct and indirect clients would depend on it to securely maintain sensitive and

valuable Private Information of Plaintiff George and Nebraska Class Members. Progress accepted the responsibility of protecting this Private Information from unauthorized disclosure while keeping the inadequate state of the MOVEit software's security controls secret from the public. Accordingly, because Progress represented that its MOVEit software would securely maintain their Private Information, Plaintiff George and Nebraska Class Members acted reasonably in relying on Progress's misrepresentations and omissions, the truth of which they could not have discovered.

1705. Progress intentionally, knowingly, and maliciously violated Nebraska's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff George's and Nebraska Class Members' rights.

1706. As a direct and proximate result of Progress's unfair and deceptive acts and practices, Plaintiff George and Nebraska Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1707. Progress's unfair and deceptive acts and practices complained of herein affected the public interest, including the large number of Nebraskans affected by the Data Breach.

1708. Plaintiff George and Nebraska Class Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, civil penalties, and attorneys' fees and costs.

PROGRESS BELLWETHER TWENTY-FOURTH CLAIM FOR RELIEF
New Jersey Consumer Fraud Act ("NJCFA")
N.J. Stat. §§ 56:8-1, *et seq.*
(Brought by Margaret Phelan on behalf of the Progress New Jersey Class)

1709. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1710. Plaintiff Margaret Phelan brings this claim against Progress on behalf of the Progress New Jersey Class (the "New Jersey Class").

1711. Progress conducts substantial business in New Jersey. It has sought and obtained business from numerous businesses conducting business in New Jersey.

1712. The NJCFA states:

> The act, use or employment by any person of any commercial practice that is unconscionable or abusive, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice.

N.J. Stat. § 56:8-2.

1713. Plaintiff Phelan, New Jersey Class Members, and Progress are "persons" under the NJCFA. N.J. Stat. § 56:8-1(d). 233.

1714. The services that Progress provided are "merchandise" pursuant to the NJCFA. N.J. Stat. § 56:8-1(c).

1715. Progress made uniform representations to Plaintiff Phelan and New Jersey Class Members, through the users of its MOVEit software, that Plaintiff Phelan's and New Jersey Class Members' Private Information would remain private, as alleged above. Progress committed deceptive omissions in violation of the NJCFA by failing to inform Plaintiff Phelan and New

Jersey Class Members that it would not adequately secure their Private Information. Documents that should have contained such disclosures, but did not, include the privacy policies referenced in this Complaint and other statements alleged above.

1716. Progress separately engaged in unfair acts and practices in violation of the NJCFA by failing to implement and maintain reasonable security measures to protect and secure Plaintiff Phelan's and New Jersey Class Members' Private Information in a manner that complied with applicable laws, regulations, and industry standards. The failure to implement and maintain reasonable data security measures offends established public policy, is immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

1717. Due to the Data Breach, Plaintiff Phelan and New Jersey Class Members have lost property in the form of their Private Information. Further, Progress's failure to adopt reasonable practices in protecting and safeguarding their Private Information will force Plaintiff Phelan and New Jersey Class Members to spend time or money to protect against identity theft.

1718. Plaintiff Phelan and New Jersey Class Members are now at a substantially higher risk of medical identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Progress's practice of collecting and storing Private Information without appropriate and reasonable safeguards to protect such information.

1719. Plaintiff Phelan and New Jersey Class Members were damaged by Progress's violation of the NJCFA because: (i) they paid—through the users of MOVEit software—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—a risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their Private Information was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their Private Information has been breached; (v) they were

deprived of the value of their Private Information, for which there is a well-established national and international market; (vi) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) they overpaid for the services that were received without adequate data security.

PROGRESS BELLWETHER TWENTY-FIFTH CLAIM FOR RELIEF
New York Deceptive Trade Practices Act ("GBL")
N.Y. Gen. Bus. Law. § 349
(Brought by Barbara Cruciata, Michelle Gonsalves, Gilbert Hale, Lynda Hale, and Margaret Kavanagh on behalf of the Progress New York Class)

1720. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1721. Plaintiffs Barbara Cruciata, Michelle Gonsalves, Gilbert Hale, Lynda Hale, and Margaret Kavanagh (collectively, the "Progress New York Plaintiffs") bring this claim against Progress on behalf of the Progress New York Class (the "New York Class").

1722. Progress engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect the Progress New York Plaintiffs' and New York Class Members' Private Information, which was a direct and proximate cause of the Data Breach, the Progress New York Plaintiffs' and New York Class Members' Private Information being compromised, and subsequent harms caused to Progress New York Plaintiffs and New York Class Members;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures, despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach, the Progress New York Plaintiffs' and New York Class Members' Private Information being compromised, and subsequent harms caused to the Progress New York Plaintiffs and New York Class Members;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of the Progress New York Plaintiffs' and New York Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902 which was a direct and proximate cause of the Data Breach, the

Progress New York Plaintiffs' and New York Class Members' Private Information being compromised, and subsequent harms caused to the Progress New York Plaintiffs and New York Class Members;

d. Misrepresenting that it would protect the privacy and confidentiality of the Progress New York Plaintiffs' and New York Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of the Progress New York Plaintiffs' and New York Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure the Progress New York Plaintiffs' and New York Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of the Progress New York Plaintiffs' and New York Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902.

h. Progress's representations and omissions were material because they were likely to deceive reasonable consumers and clients about the adequacy of their respective data security policies and practices and ability to protect the confidentiality of consumers' Private Information.

1723. Accordingly, the Progress New York Plaintiffs and New York Class Members acted reasonably in relying on Progress's misrepresentations and omissions, the truth of which they could not have discovered.

1724. Progress acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded the Progress New York Plaintiffs and New York Class Members' rights.

1725. As a direct and proximate result of Progress's unfair, unlawful, and/or fraudulent acts and practices, the Progress New York Plaintiffs and New York Class Members have suffered

and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including, but not limited to, fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for the services of direct users, vendors, vendor contracting entities, and vendor contracting entity customers who utilized MOVEit software; loss of the value of access to their Private Information; value of identity and credit protection and repair services made necessary by the Data Breach; and they face ongoing risks of future harms insofar as they have yet to implement the necessary policies, practices, and measures to adequately safeguard their Private Information in compliance with laws and industry standards.

1726. Progress's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the many New Yorkers affected by the Data Breach.

1727. The above deceptive and unlawful practices and acts by Progress caused substantial injury to the Progress New York Plaintiffs and New York Class Members that they could not reasonably avoid.

1728. The Progress New York Plaintiffs and New York Class Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorneys' fees and costs.

PROGRESS BELLWETHER TWENTY-SIXTH CLAIM FOR RELIEF
North Carolina Identity Theft Protection Act
N.C. Gen. Stat. Ann. § 75-1.1
(Brought by Ben Dieck on behalf of the Progress North Carolina Class)

1729. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1730. Plaintiff Ben Dieck brings this claim against Progress on behalf of the Progress North Carolina Class (the "North Carolina Class").

1731. Progress is a business that owns or licenses computerized data that includes Private Information as defined by N.C. Gen. Stat. § 75- 61(1).

1732. Plaintiff Dieck and North Carolina Class Members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

1733. Progress is required to accurately notify Plaintiff Dieck and North Carolina Class Members if it discovers a security breach or receives notice of a security breach (where Private Information that is or has been unencrypted and unredacted was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. § 75-65.

1734. Plaintiff Dieck's and North Carolina Class Members' Private Information includes information as covered under N.C. Gen. Stat. § 75-61(10).

1735. Because Progress discovered a security breach and had notice of a security breach (where unencrypted and unredacted Private Information was accessed or acquired by unauthorized persons), Progress had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

1736. By failing to disclose the Data Breach in a timely and accurate manner, Progress violated N.C. Gen. Stat. § 75-65.

1737. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. Art. 2A § 75-1.1.

1738. As a direct and proximate result of Progress's violations of N.C. Gen. Stat. § 75-65, Plaintiff Dieck and North Carolina Class Members suffered damages, as alleged above.

1739. Plaintiff Dieck and North Carolina Class Members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorneys' fees.

PROGRESS BELLWETHER TWENTY-SEVENTH CLAIM FOR RELIEF
North Carolina Unfair and Deceptive Trade Practices Act
N.C. Gen. Stat. Ann. § 75-1.1, *et seq.*
(Brought by Ben Dieck on behalf of the Progress North Carolina Class)

1740. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1741. Plaintiff Ben Dieck brings this claim against Progress on behalf of the Progress North Carolina Class.

1742. Progress advertised, offered, or sold goods or services in North Carolina and engaged in commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

1743. Progress engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Dieck's and North Carolina Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Dieck's and North Carolina Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Dieck's and North Carolina Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Dieck's and North Carolina Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or properly secure Plaintiff Dieck's and North Carolina Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Dieck's and North Carolina Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

1744. Progress's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Progress's data security and ability to protect the confidentiality of consumers' Private Information.

1745. Progress intended to mislead Plaintiff Dieck and North Carolina Class Members and induce them to rely on its misrepresentations and omissions.

1746. Had Progress disclosed to Plaintiff Dieck and North Carolina Class Members that its MOVEit software was not secure and, thus, vulnerable to attack, Progress would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Progress was trusted with sensitive and valuable Private Information regarding millions of consumers via its MOVEit software, including Plaintiff Dieck and North Carolina Class Members. Progress accepted the responsibility of protecting the data held on its MOVEit software while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Dieck and North Carolina Class Members acted reasonably in relying on Progress's misrepresentations and omissions, the truth of which they could not have discovered.

1747. Progress acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff Dieck's and North Carolina Class Members' rights.

1748. As a direct and proximate result of Progress's unfair and deceptive acts and practices, Plaintiff Dieck and North Carolina Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including, but not limited to, fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Progress's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

1749. Progress's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

1750. Plaintiff Dieck and North Carolina Class Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

PROGRESS BELLWETHER TWENTY-EIGHTH CLAIM FOR RELIEF
Ohio Consumer Sales Practices Act
Ohio Rev. Code § 1345.01, *et seq.*
(Brought by Elaine McCoy on behalf of the Progress Ohio Class)

1751. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1752. Plaintiff Elaine McCoy brings this claim against Progress on behalf of the Progress Ohio Class (the "Ohio Class").

1753. Progress, while operating in Ohio, engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code § 1345.01(A) and (B). This includes but is not limited to the following:

a. failing to enact adequate privacy and security measures to protect Plaintiff McCoy and the Ohio Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. failing to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. knowingly and fraudulently misrepresenting that its MOVEit software would maintain adequate data privacy and that its security practices and procedures would safeguard Plaintiff McCoy and the Ohio Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft;

d. omitting, suppressing, and concealing the material fact of the inadequacy of its MOVEit software's privacy and security protections for Plaintiff McCoy's and the Ohio Class Members' Private Information;

e. knowingly and fraudulently misrepresenting that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff McCoy and the Ohio Class Members' Private Information, including, but not limited to, duties imposed by the FCRA, 15. U.S.C.§ 1681e, and the GLBA, 15 U.S.C. § 6801 et seq.;

f. failing to maintain the privacy and security of Plaintiff McCoy and the Ohio Class Members' Private Information, in violation of duties imposed by applicable federal and state laws, including, but not limited to, those mentioned in the aforementioned paragraph, directly and proximately causing the Data Breach; and

g. failing to disclose the Data Breach to Plaintiff McCoy and the Ohio Class Members in a timely and accurate manner, in violation of the duties imposed by Ohio Rev. Code § 1349.19(B).

1754. As a direct and proximate result of Progress's practices, Plaintiff McCoy and the Ohio Class Members suffered injury and/or damages, including, but not limited to, time and

expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Private Information.

1755. The above unfair and deceptive acts and practices by Progress were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff McCoy and the Ohio Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

1756. Progress knew or should have known that its MOVEit software and its data security practices were inadequate to safeguard Plaintiff McCoy's and the Ohio Class Members' Private Information and that risk of a data breach or theft was highly likely. The actions of Progress in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

1757. Pursuant to Ohio Rev. Code § 1345.09, Plaintiff McCoy and the Ohio Class Members seek an order enjoining Progress's unfair and/or deceptive acts or practices actual damages – trebled (to be proven at the time of trial), and attorneys' fees, costs, and any other just and proper relief, to the extent available under the Ohio Consumer Sales Practices Act, Ohio Rev. Code §§ 1345.01, *et seq*.

PROGRESS BELLWETHER TWENTY-NINTH CLAIM FOR RELIEF
Violations of the Pennsylvania Unfair Trade Practices and Consumer Protection Law ("UTPCPL")
73 P.S. §§ 201-1–201-9.3
(*Brought by Steven Checchia, Marvin Dovberg, and Victor Diluigi on behalf of the Progress Pennsylvania Class)*

1758. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1759. Plaintiffs Checchia, Dovberg, and Diluigi (collectively, the "Progress Pennsylvania Plaintiffs") bring this claim against Progress on behalf of the Progress Pennsylvania Class (the "Pennsylvania Class").

1760. Progress sells and performs services in the Commonwealth of Pennsylvania.

1761. The Progress Pennsylvania Plaintiffs, Pennsylvania Class Members, and Progress are "persons" as defined by the UTPCPL. 73 P.S. § 201-2(2).

1762. Progress's products and services constitute as "trade" and "commerce" under the statute. 73 P.S. § 201-2(3).

1763. Users of Progress's MOVEit software obtained Progress Pennsylvania Plaintiffs' and Pennsylvania Class Members' Private Information in connection with the services they perform and provide.

1764. Progress engaged in unfair or deceptive acts in violation of the UTPCPL by failing to implement and maintain reasonable security measures to protect and secure consumers' (such as Progress Pennsylvania Plaintiffs' and Pennsylvania Class Members') Private Information in a manner that complied with applicable laws, regulations, and industry standards, including by failing to develop and maintain MOVEit as a secure file-transfer protocol software, such that it failed to ensure the safety of consumers' data that was collected, stored, or transferred via Progress's MOVEit software.

1765. As alleged above, Progress, through its direct and indirect customers, made explicit statements to consumers that their Private Information will remain private and secure.

1766. The UTPCPL lists twenty-one instances of "unfair methods of competition" and "unfair or deceptive acts or practices." 73 P.S. § 201-2(4). Progress's failure to adequately protect Progress Pennsylvania Plaintiffs' and Pennsylvania Class Members' Private Information while

holding out that it would adequately protect the Private Information falls under at least the following categories:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation or connection that he does not have (73 P.S. § 201-2(4)(v));

b. Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model, if they are of another (73 P.S. § 201-2(4)(vii));

c. Advertising goods or services with intent not to sell them as advertised (73 P.S. § 201-2(4)(ix)); and

d. Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding (73 P.S. § 201-2(4)(xxi)).

1767. Due to the Data Breach, Progress Pennsylvania Plaintiffs and Pennsylvania Class Members have lost property in the form of their Private Information. Further, Progress's failure to adopt reasonable practices in protecting and safeguarding their customers' Private Information will force Progress Pennsylvania Plaintiffs and Pennsylvania Class Members to spend time or money to protect against identity theft. Progress Pennsylvania Plaintiffs and Pennsylvania Class Members are now at a higher risk of identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Progress's practice of developing and maintaining MOVEit software without appropriate and reasonable safeguards to protect consumers' sensitive and nonpublic Private Information.

1768. As a result of Progress's violations of the UTPCPL, Progress Pennsylvania Plaintiffs and Pennsylvania Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased or imminent risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private

Information; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market; (v) lost value of the unauthorized access to their Private Information permitted by Progress; (vi) the value of long-term credit monitoring and identity theft protection products necessitated by the Data Breach; (vii) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (viii) overpayment for the services that were received without adequate data security.

1769. Pursuant to 73 P.S. § 201-9.2(a), Progress Pennsylvania Plaintiffs seek actual damages, $100, or three times their actual damages, whichever is greatest. Progress Pennsylvania Plaintiffs also seek costs and reasonable attorney fees.

PROGRESS BELLWETHER THIRTIETH CLAIM FOR RELIEF
Vermont Consumer Fraud Act
9 V.S.A. §§ 2451, *et seq.*
(Brought by Plaintiff Patricia Marshall on behalf of the Progress Vermont Class)

1770. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1771. Plaintiff Patricia Marshall brings this claim against Progress on behalf of the Progress Vermont Class (the "Vermont Class").

1772. Progress conducts substantial business in Vermont. It has sought and obtained business from numerous businesses conducting business in Vermont.

1773. Plaintiff Marshall and the Vermont Class Members are "consumers" within the meaning of 9 V.S.A. § 2451a(a) insofar as they agree to pay for products and services from users of MOVEit software—for data security protection they did not receive from Progress.

1774. Progress is a "seller" within the meaning of 9 V.S.A. § 2451a(c).

1775. The Vermont Consumer Fraud Act ("VCFA") prohibits unfair acts or practices in the conduct of trade or commerce. In interpreting its provisions, the VCFA requires express consideration be given to interpretations by the FTC relating to § 5 of the FTC Act. *See* 9 V.S.A. § 2453(b).

1776. Progress engaged in unfair business practices prohibited by the VCFA by unreasonably adopting and maintaining data security measures that were inadequate to protect Private Information and prevent the Data Breach. These unfair practices occurred repeatedly in connection with Progress's trade or business.

1777. Progress's affirmative acts in adopting and maintaining inadequate security measures are unfair within the meaning of the VCFA because they constituted immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers, and provided no benefit to consumers or competition.

1778. Progress's failures also were unfair within the meaning of VCFA because its conduct undermined Vermont public policy that Private Information be protected from unauthorized disclosure, as reflected in 9 V.S.A. § 2435.

1779. Plaintiff Marshall and the Vermont Class Members reasonably expected Progress to develop and maintain secure file-transfer software, adhere to industry standards, and otherwise use reasonable care to protect their Private Information.

1780. Progress's conduct harmed competition. While representing that its MOVEit software had appropriate and sound data security in place, Progress cut corners and minimized costs. Meanwhile, its competitors spent the time and money necessary to ensure private information was appropriately secured and safeguarded. Further, the injuries suffered by Plaintiff Marshall and the Vermont Class Members are not outweighed by any countervailing benefits to

consumers or competition. Moreover, there is no way Plaintiff Marshall and the Vermont Class Members could have known about Progress's inadequate data security practices or avoided the injuries they sustained. There were commercially viable measures Progress could have taken to mitigate the risks of any data breach while furthering Progress's legitimate business interests, other than its conduct responsible for the Data Breach.

1781. Plaintiff Marshall and the members of the Vermont Class Members are located in Vermont and suffered an injury in Vermont.

1782. Progress willfully engaged in the unfair acts and practices described above and knew or should have known that those acts and practices were unfair in violation of the VCFA.

1783. As a direct and proximate result of Progress's unfair practices and violation of the VCFA, Plaintiff Marshall and the Vermont Class Members have suffered and will continue to suffer substantial injury and ascertainable loss and are entitled to equitable and such other relief as this Court considers necessary and proper.

PROGRESS BELLWETHER THIRTY-FIRST CLAIM FOR RELIEF
Washington Data Breach Notification Law
Wash. Rev. Code §§ 19.255.010, *et seq.*
(Brought by Plaintiff Megan McClendon on behalf of the Progress Washington Class)

1784. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1785. Plaintiff Megan McClendon brings this claim against Progress on behalf of the Progress Washington Class (the "Washington Class").

1786. Progress, as an entity that facilitates and/or takes responsibility for the collection, handling, dissemination, and other dealings with nonpublic Private Information (as defined by Wash. Rev. Code § 19.255.005(2)(a)), Progress is subject to the notice requirements of Wash. Rev. Code § 19.255.010(1).

1787. Plaintiff McClendon and Washington Class Members' Private Information includes "Private Information" as defined by Wash. Rev. Code § 19.255.005(2)(a).

1788. In accordance with Washington law, Progress, as a business that owns, licenses, or maintains computerized data that includes "Private Information," was required to accurately notify Plaintiff McClendon and Washington Class Members of the Data Breach affecting its MOVEit software data security system if Private Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, in the most expedient time possible and without unreasonable delay pursuant to Wash. Rev. Code §§ 19.255.010(1), (2).

1789. The Data Breach described herein constituted a "breach of the security of the system" of Progress as defined by Wash. Rev. Code § 19.255.005(1).

1790. Because Progress knew and/or reasonably believed that Plaintiff McClendon's and Washington Class Members' Private Information was acquired by unauthorized persons during the Data Breach, Progress had an obligation to disclose the Data Breach in a timely and accurate fashion.

1791. Upon information and belief, as a proximate result of Progress's failures to maintain its MOVEit software, Plaintiff McClendon's and Washington Class Members' Private information was not secured and was accessed or compromised by CL0P during the Data Breach.

1792. As alleged above, Progress unreasonably delayed informing Plaintiff McClendon and Washington Class Members about the Data Breach, affecting their Private Information, after Progress knew that the Data Breach had occurred.

1793. By failing to disclose the Data Breach in the most expedient time possible and without unreasonable delay, Progress violated Wash. Rev. Code §§ 19.255.010(1), (2).

1794. As a result of Progress's violation of Wash. Rev. Code §§ 19.255.010(1), (2), Plaintiff McClendon and Washington Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff McClendon and Washington Class Members because their stolen Private Information would have had less value to identity thieves.

1795. As a result of Progress's violation of Wash. Rev. Code §§ 19.255.010(1), (2), Plaintiff McClendon and Washington Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

1796. As a direct and proximate result of Progress' violations of Wash. Rev. Code §§ 19.255.010(1), (2), Plaintiff McClendon and Washington Class Members suffered damages, as described above.

1797. Plaintiff McClendon and Washington Class Members seek relief under Wash. Rev. Code §§ 19.255.010(1), (2) for the harm they suffered due to Progress's willful violations of Wash. Rev. Code §§ 19.255.040(3)(a), (b), including actual damages, equitable relief, costs, and attorneys' fees.

PROGRESS BELLWETHER THIRTY-SECOND CLAIM FOR RELIEF
Washington Consumer Protection Act
Wash. Rev. Code §§ 19.86.020, *et seq.*
(Brought by Plaintiff Megan McClendon on behalf of the Progress Washington Class)

1798. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1799. Plaintiff Megan McClendon brings this claim against Progress on behalf of the Progress Washington Class.

1800. Progress is a "person" as defined by Wash. Rev. Code Ann. § 19.86.010(1).

1801. Progress advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

1802. Progress engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

a. Failing to implement and maintain reasonable security and privacy measures with regard to its MOVEit software in order to protect Plaintiff McClendon's and Washington Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff McClendon's and Washington Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that its MOVEit software would protect the privacy and confidentiality of Plaintiff McClendon's and Washington Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff McClendon's and Washington Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and 42 U.S.C. § 1320d;

f. Failing to timely and adequately notify the Plaintiff McClendon and Washington Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff McClendon's and Washington Class Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff McClendon's and Washington Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d.

1803. Progress's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Progress's data security and the ability of Progress's MOVEit software to protect the confidentiality of consumers' Private Information.

1804. Progress acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff McClendon's and Washington Class Members' rights. Progress is of such a sophisticated and large nature that other data breaches and public information regarding security vulnerabilities put it on notice that the security and privacy protections provided by its MOVEit software were inadequate.

1805. Progress's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, its conduct affected the public interest, including the many Washingtonians affected by the Data Breach.

1806. As a direct and proximate result of Progress's unfair and deceptive acts and practices, Plaintiff McClendon and Washington Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

1807. Plaintiff McClendon and Washington Class Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

PROGRESS BELLWETHER THIRTY-SEVENTH CLAIM FOR RELIEF
Declaratory Judgment
28 U.S.C. §§ 2201, *et seq.*
(Brought by Plaintiffs on behalf of the Progress Nationwide Class, or, in the alternative, Progress State Classes, against Progress)

1808. Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

1809. All Bellwether Plaintiffs bring this claim against Progress on behalf of the Progress Nationwide Class or, in the alternative, the Progress State Classes.

1810. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

1811. Progress owed a duty of care to Plaintiffs and Progress Bellwether Class Members, which required it to develop and maintain software that would adequately safeguard Plaintiffs' and Progress Bellwether Class Members' Private Information.

1812. The Private Information belonging to Plaintiffs and Progress Bellwether Class Members remains on MOVEit software.

1813. Upon information and belief, Progress's data security measures on its MOVEit software remain inadequate.

1814. Furthermore, Plaintiffs and Progress Bellwether Class Members continue to suffer injury as a result of the compromise of their Private Information, and the risk remains that further compromises of their Private Information will occur in the future.

1815. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Progress owes a legal duty to secure the MOVEit software, and thereby secure Plaintiffs' and Progress Bellwether Class Members' Private Information under the common law, HIPAA, the FTCA, and other state and federal laws and regulations, as set forth herein;

b. Progress's existing data monitoring measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect individuals' Private Information; and

c. Progress continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiffs' and Progress Bellwether Class Members' Private Information.

1816. This Court should also issue corresponding prospective injunctive relief requiring Progress to employ adequate security protocols consistent with legal and industry standards to protect members' Private Information, as described in the Prayer for Relief.

1817. If an injunction is not issued, Plaintiffs and Progress Bellwether Class Members will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach of Progress's systems. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs and Progress Bellwether Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable and they will be forced to bring multiple lawsuits to rectify the same conduct.

1818. The hardship to Plaintiffs and Progress Bellwether Class Members if an injunction is not issued exceeds the hardship to Progress if an injunction is issued. Among other things, if another massive data breach occurs at Progress, Plaintiffs and Progress Bellwether Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Progress of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Progress has a pre-existing legal obligation to employ such measures.

1819. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach of Progress's MOVEit software, thus preventing future injury to Plaintiffs and Progress Bellwether Class Members whose Private Information would be further compromised.

IV. PRAYER FOR RELIEF AS AGAINST PROGRESS

1820. Plaintiffs, individually and on behalf of the Progress Bellwether Class, respectfully request that the Court grant the following relief:

a. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiffs as Class Representative and undersigned counsel as Class Counsel;

b. Find in favor of Plaintiffs and the Classes on all counts asserted herein;

c. Award Plaintiffs and the Classes actual, statutory, and/or punitive monetary damages to the maximum extent as allowed by law;

d. Award Plaintiffs and the Classes compensatory, consequential, general, and/or nominal monetary damages in an amount to be proven at trial;

e. Award Plaintiffs and the Classes restitution and all other applicable forms of equitable monetary relief;

f. Award Plaintiffs and the Classes equitable relief by enjoining Progress from engaging in the wrongful conduct complained of herein regarding the misuse or disclosure of the private information of Plaintiffs and Class Members, and by requiring Progress to issue prompt, complete, and accurate disclosure to Plaintiffs and Class Members;

g. Award Plaintiffs and the Classes injunctive relief as permitted by law or equity to assure that they have an effective remedy, and to protect the interests of Plaintiffs and Class Members, including, but not limited to, an order:

i. requiring Progress to protect from unauthorized disclosure all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws, including by adequate encryption of all such data and by preventing unauthorized access to decryption keys;

ii. requiring Progress to delete, destroy, and purge any personal identifying information of Plaintiffs and Class Members in its

possession unless Progress can provide to the Court reasonable justification for the retention and use of such information when weighted against the privacy interests of Plaintiffs and Class Members;

iii. requiring Progress to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Progress's systems on a periodic basis, and ordering Progress to promptly correct any problems or issues detected by such third-party security auditors;

iv. requiring Progress to engage independent third-party security auditors and internal personnel to run automated security monitoring including, but not limited to, regular database scanning and securing checks;

v. requiring Progress to audit, test, and train its security personnel regarding any new or modified procedures;

vi. requiring Progress to segment data by, among other things, creating firewalls and access controls so that if one area of Progress's network is compromised, hackers cannot gain access to other portions of Progress's systems;

vii. requiring Progress to establish for all Progress employees an information security training program that includes annual training, with additional training to be provided as appropriate;

viii. requiring Progress to establish for all Progress security personnel a security training program that includes regularly scheduled internal training and education to inform Progress' internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

ix. requiring Progress to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Progress's policies, programs, and systems for protecting personal identifying information;

x. requiring Progress to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Progress's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xi. requiring Progress to provide notice to Plaintiffs and all Class Members regarding the full nature and extent of the Data Breach and the disclosure of Private Information to unauthorized persons, including the threat posed as a result of the disclosure of their confidential personal information, and educating Plaintiffs and Class Members regarding steps affected individuals should take to protect themselves;

xii. requiring Progress to implement logging and monitoring programs sufficient to track traffic to and from Progress's servers;

xiii. requiring, for a period of 10 years, the appointment of a qualified and independent third-party assessor to conduct an annual SOC 2 Type 2 attestation to evaluate Progress's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Classes, and to report any deficiencies with compliance of the Court's final judgment;

xiv. requiring Progress to implement multi-factor authentication requirements, if not already implemented; and

xv. requiring Progress's employees to employ passwords consistent with best security practices and to change their passwords on a timely and regular basis.

h. Award disgorgement and restitution of all earnings, profits, compensation, and benefits received by Progress as a result of its unlawful acts;

i. Order Progress to purchase or provide funds for lifetime credit monitoring and identify theft insurance to Plaintiffs and Class Members;

j. Order Progress to pay all costs necessary to notice Class Members about the judgment and all costs necessary to administer a court approved claims process.

k. Award Plaintiffs and the Classes pre-judgment and post-judgment interest to the maximum extent allowed by law;

l. Grant Plaintiffs and the Classes leave to amend this complaint to conform to the evidence produced during the course of this case;

m. Award Plaintiffs and the Classes reasonable attorneys' fees, costs, and expenses, as allowable;

n. Where necessary, distribute any monies recovered from Progress on behalf of Class Members or the general public via fluid recovery or cy pres recovery as applicable to prevent Progress from retaining benefits of its wrongful conduct;

o. Award Plaintiffs and the Class such other favorable relief as allowable under law or at equity;

p. Award any other and further relief as may be just and proper; and

q. Conduct a trial by jury on all issues so triable.

CHAPTER THREE:

FACTUAL ALLEGATIONS AND CAUSES OF ACTION AGAINST PBI

1821. The PBI Bellwether Plaintiffs (relisted for ease of review) Keith Bailey, Camille Burgan, Eugene Burgan, Steven Checchia, Gilbert Hale, Lynda Hale, Brinitha Harris, Patrice Hauser, Tricia Hernandez, Patricia Marshall, Rita Pasquarelli, Margaret Phelan, Jose Soto, Steven Teppler, and Katharine Uhrich, individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to themselves, allege as follows against the PBI Bellwether Defendants (relisted for ease of review) PBI, Genworth Defendants, TIAA, Milliman Defendants, and MLIC:

I. Overview of the PBI Bellwether Defendants

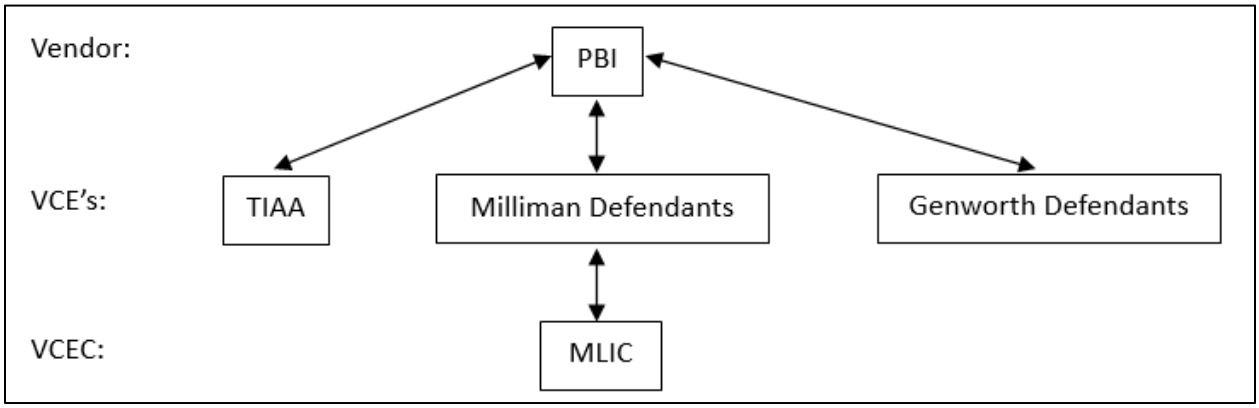
1822. The MOVEit Transfer software is owned and operated by Progress and used by more than 1,700 companies and 3.5 million users worldwide, including by PBI and the PBI Bellwether Defendants in the ordinary course of their businesses, either directly or indirectly.

1823. PBI is a for-profit Delaware corporation with its principal place of business in Minneapolis, Minnesota. PBI is a pension plan "sponsor, administrator, or record keeper" "for thousands of organizations" and pension plans.[453] In the ordinary course of its business, PBI uses Progress's MOVEit service to store large amounts of data provided (or otherwise possessed/maintained) by its customers, including Defendants GLAIC, GLIC, Genworth Financial, Milliman Inc., Milliman Solutions, MLIC, and TIAA (collectively, "PBI-Contracting Defendants").[454]

[453] PBI, *Homepage*, https://www.pbinfo.com/ (last accessed Nov. 27, 2024).

[454] PBI, *Global MOVEit Transfer Cyberattack*, https://www.pbinfo.com/faq-communication/ (last accessed Oct. 21, 2024).

1824. Specifically, in documents filed with this Court, PBI characterizes itself as a "vendor" of the MOVEit service. *See* ECF No. 1161-1 at 4. Defendants GLAIC, GLIC, Genworth Financial, Milliman Inc., Milliman Solutions, and TIAA characterize themselves as "vendor contracting entities" that use PBI's vendor services. *See id*. at 5-6. Defendant MLIC characterizes itself as a "vendor contracting entity customer," that uses services provided by Milliman, which is utilizing PBI as its vendor. *See id.* at 5. Below is a chart showing this interplay:



Thus, through these relationships, all PBI-Contracting Defendants used PBI as their vendor, either directly or indirectly, and in the ordinary course of their business shared, transmitted, or otherwise maintained their customers' highly sensitive information with PBI or otherwise made it accessible to PBI through MOVEit (including, but not limited to, customers' Social Security numbers, first and last names, dates of birth, addresses, genders, and/or life insurance policy numbers (collectively referred to hereinafter as "PII")).

1825. Defendant Genworth Financial is a publicly traded, Fortune 500 company, Delaware corporation, with its principal place of business in Richmond, Virginia. Genworth Financial markets mortgages, long-term care insurance, life insurance, and other insurance and financial products, primarily to individual consumers.[455] Defendant GLAIC is a subsidiary of

[455] Genworth Financial, Inc., Annual Report (Form 10-K) *SEC Form 10-K* (Feb. 28, 2023).

Genworth Financial with its principal place of business in Richmond, Virginia. Defendant GLIC is a subsidiary of Genworth Financial with its principal place of business in Richmond, Virginia. Genworth Defendants contract with PBI "to satisfy regulatory obligations to scan social security data to determine whether a policyholder may have passed and triggered death benefits under a life insurance policy or annuity contract."[456] Genworth Defendants "also use[s] PBI to identify deaths that have occurred across [Genworth's] other lines of insurance, as well as the deaths of insurance agents to whom [Genworth] pay[s] commissions."[457]

1826. Defendant Milliman Inc. is a Washington corporation with its principal place of business in Seattle, Washington. Milliman Inc. provides administrative services to employee benefit and pension plan sponsors.[458] Defendant Milliman Solutions is a subsidiary of Milliman, Inc. with its principal place of business in Seattle, Washington. Milliman Solutions markets its business as providing risk assessment services to clients, including life insurance companies.[459]

---

[456] *MOVEit Security Event*, Genworth (last updated Aug. 31, 2023), https://www.genworth.com/moveit#backgroundinfo.

[457] *See, e.g.*, Genworth, *Data Breach Notice Letter to Impacted Living Residents of Rhode Island* (July 31, 2023), https://a-us.storyblok.com/f/1008916/0db43daf1b/genworth-consumer-notice_ri.pdf; *MOVEit Security Event*, Genworth (last updated Aug. 31, 2023), https://www.genworth.com/moveit#backgroundinfo.; *see also* Genworth, *Genworth Financial Inc. SEC Form 8-K*, June 16, 2023, https://www.sec.gov/Archives/edgar/data/1276520/000119312523172549/d463993d8k.htm ("[Genworth's] life insurance businesses use PBI to, among other things, satisfy applicable regulatory obligations to search various databases to identify the deaths of insured persons under life insurance policies, and to identify the deaths of insured persons under long-term care insurance, and annuity policies which can impact premium payment obligations and benefit eligibility. For life insurance policies and annuity contracts, this helps identify the possible eligibility of beneficiaries for death benefits even prior to the submission of claims, or for policies that beneficiaries may not know exist.").

[458] *Data Breach Notifications – Milliman Solutions LLC*, Office of the Maine Attorney General (July 17, 2023), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a98d9ae9-b898-4aaa-8dde-de04551aaedb.shtml.

[459] *Data Breach Notifications – Milliman Solutions LLC*, Office of the Maine Attorney General (July 17, 2023), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a98d9ae9-b898-4aaa-8dde-de04551aaedb.shtml.

Milliman Defendants provide administrative and risk assessment services to a global customer base – including "insurers, healthcare organizations, governments, and employers"[460], such as PBI Bellwether Defendant MLIC. "As part of those services, [Milliman] utilizes . . . [PBI] to conduct research on whether consumers have passed away. For that purpose, [Milliman] transferred data regarding its clients' consumers to PBI utilizing a secure and encrypted file transfer protocol."[461]

1827. Defendant MLIC is an Iowa corporation with its principal place of business in Madison, Wisconsin, that operates as an insurance company offering life, accidental, and health insurance throughout the United States.[462] In the ordinary course of its business, MLIC pays to utilize services offered by Milliman Defendants.

1828. Defendant TIAA is a New York based stock insurance company with its principal place of business in New York, New York. TIAA provides services to over 5 million clients from more than 15,000 institutions and manages nearly $1 trillion in assets with holdings in more than 50 countries. In the ordinary course of its business, "TIAA utilizes [PBI] to assist with death claim and beneficiary processes."[463]

1829. PBI Bellwether Defendants owed duties to PBI Bellwether Plaintiffs and PBI Bellwether Class Members (defined below) to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and

---

[460] Milliman, *Our mission*, https://www.milliman.com/en/our-story (last accessed Oct. 24, 2024).

[461] *Data Breach Notifications – Milliman Solutions LLC*, Office of the Maine Attorney General (July 17, 2023), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a98d9ae9-b898-4aaa-8dde-de04551aaedb.shtml.

[462] MEMBERS Life Insurance Co., Bloomberg, https://www.bloomberg.com/profile/company/11789Z:US?embedded-checkout=true (last accessed Nov. 27, 2024).

[463] *Notice of Data Security Incident*, TIAA (July 21, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/ed67df63-aced-4ecb-91ce-602c7e34c83a/573351f0-74fc-4e19-9a62-a51fb837a3bb/Regulator%20Notice%20-%20TIAA%20ME%20AG.pdf.

disclosure. PBI Bellwether Defendants breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the PII entrusted to them from unauthorized access and disclosure.

1830. As a result of PBI Bellwether Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred and PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII was accessed by, and disclosed to, an unauthorized third-party actor. PBI Bellwether Plaintiffs thus bring this complaint on behalf of themselves, and all similarly situated individuals whose PII was exposed as a result of the Data Breach, which PBI Bellwether Defendants learned of on or about May 27, 2023, but PBI[464], Genworth Defendants[465], Milliman Defendants[466], and TIAA[467] did not publicly disclose until approximately July 2023.

A. Nature of PBI's Business

1831. PBI performs various data verification, death audit, and participant location services for insurance companies, pension funds, financial institutions, government entities, and other businesses, including the PBI Bellwether Defendants.[468]

[464] *Data Breach Notifications – Pension Benefit Information, LLC,* Office of the Maine Attorney General (July 12, 2023), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/14efac97-4a7c-4322-98eb-2e953884eb58.shtml.

[465] *MOVEit Security Event*, Genworth (last updated Aug. 9, 2023), https://www.genworth.com/moveit.

[466] *Data Breach Notifications – Milliman Solutions LLC*, Office of the Maine Attorney General (July 17, 2023), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a98d9ae9-b898-4aaa-8dde-de04551aaedb.shtml.

[467] *Data Breach Notifications – TIAA*, Office of the Maine Attorney General (July 14, 2023), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/ed67df63-aced-4ecb-91ce-602c7e34c83a.shtml.

[468] PBI, *Privacy Policy*, https://www.pbinfo.com/privacy-policy/ (last accessed Oct. 18, 2024).

1832. PBI claims it "provides thousands of organizations with the best population management solutions in the industry."[469]

1833. PBI's services and products require that its business clients—including the PBI Bellwether Defendants—provide PBI with their customers' and policyholders' sensitive PII.[470]

1834. According to PBI, "[p]ersonal information is provided to PBI from or on behalf of [its business clients], and PBI is a service provider, contractor, or data processor/collector to such organizations."[471]

1835. PBI solicits and collects sensitive consumer data from its business clients—including the PBI Bellwether Defendants—and then stores, validates, and updates that data to help them "locate people who may be eligible for benefits[,]" and "prevent[] fraud or avoid[] overpayment of benefits to deceased individuals."[472]

1836. For example, PBI conducts Social Security Death Master Index searches for its insurance company and pension fund clients.[473] In order to perform these searches, which are

[469] PBI, *We Find the Hardest to Find People*, https://www.pbinfo.com/ (last accessed Oct. 18, 2024).

[470] Resource for PBI / MOVEit Transfer Breach, Ullico, https://www.ullico.com/resource-for-pbi-moveit-transfer-breach/ (last accessed Oct. 21, 2024); see also PBI, Beyond the Numbers Part 1: Putting Participants First in Retirement Planning featuring MEA, YouTube (June 27, 2023), https://www.youtube.com/watch?v=wTC2Ers4AJM.

[471] PBI, *Privacy Policy*, https://www.pbinfo.com/privacy-policy/ (last accessed Oct. 18, 2024) ("Where personal information is provided to PBI by those organizations, PBI is a data processor, service provider or contractor to such organizations, as those terms are used in applicable privacy laws.").

[472] PBI, *Privacy Policy*, https://www.pbinfo.com/privacy-policy/ (last accessed Oct. 18, 2024).

[473] PBI, *CertiDeath*, https://www.pbinfo.com/death-audit/ (last accessed Oct. 26, 2024).

required by state law, companies must share their policyholders' sensitive PII, including Social Security numbers, with PBI.[474]

1837. PBI boasts that its services "have uncovered over $1 billion in overpayments, releasing billions in unnecessary funding liability[.]"[475]

1838. In addition to helping its business clients save money by reducing financial losses, PBI promises clients and potential clients that, by using PBI's services, "[a]s a plan sponsor, administrator, or record keeper you can be confident you're doing what's best for your plan, participants, beneficiaries and policy holders."[476]

B. PBI Bellwether Defendants used the MOVEit Transfer software to transfer and store the PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII.

1839. PBI uses the MOVEit Transfer software to facilitate the transfer and storage of its business clients' sensitive consumer data[477], including that of the PBI-Contracting Defendants (Genworth Defendants, Milliman Defendants, TIAA, and MLIC).

---

[474] *Resource for PBI / MOVEit Transfer Breach*, Ullico, https://www.ullico.com/resource-for-pbi-moveit-transfer-breach/ (last accessed Oct. 21, 2024); *see also* PBI, *CertiDeath*, https://www.pbinfo.com/death-audit/ (last accessed Oct. 26, 2024).

[475] PBI, *We Find the Hardest to Find People*, https://www.pbinfo.com/ (last accessed Oct. 18, 2024).

[476] PBI, *We Find the Hardest to Find People*, https://www.pbinfo.com/ (last accessed Oct. 18, 2024).

[477] *See* PBI, *Global MOVEit Transfer Cyberattack*, https://www.pbinfo.com/faq-communication/ (last accessed Oct. 21, 2024) ("PBI Research Services uses Progress Software's MOVEit file transfer application with some of our clients. At the end of May, Progress Software identified a cyberattack in their MOVEit software that did impact a small percentage of our clients who use the MOVEit administrative portal software resulting in access to private records."); *see also* Jill McKeon, *MOVEit Transfer Cyberattack Impacts 1.2M at Pension Benefit Information*, TechTarget (July 18, 2023), https://www.techtarget.com/healthtechsecurity/news/366594250/MOVEit-Transfer-Cyberattack-Impacts-12M-at-Pension-Benefit-Information.

1840. The PBI-Contracting Defendants provided the PBI Bellwether Plaintiffs' and Class Members' highly sensitive PII to PBI by uploading files[478] to PBI's MOVEit Transfer server using PBI's "MOVEit administrative portal software."[479]

1841. PBI claims that "[p]rotecting and securing the information of [its] clients and [the] company is of critical importance to PBI. We recognize that all relationships with current and prospective clients are based upon integrity and trust, and we take our role as custodians of confidential information very seriously."[480]

C. PBI knew it had duties to protect the PBI Bellwether Plaintiffs' and Class Members' PII, and assured them that it would.

1842. Similar to the various statements on Progress's website assuring consumers that Progress will protect their sensitive PII, PBI's website also claims that it has robust systems and processes in place to protect and secure the highly sensitive PII that it solicits, collects, stores, and maintains.

1843. In a set of "Privacy Principles"[481] published on PBI's website, PBI professes its "commit[ment] to the responsible use of information and protection of individual privacy

---

[478] PBI, Resources – Recently Recorded Webinars: Beyond the Numbers Part 1: Putting Participants First in Retirement Planning Featuring MEA, YouTube (June 27, 2023), https://www.youtube.com/watch?v=wTC2Ers4AJM at 32:10 (Jeff Anderson, Business Development Manager at PBI Research Services: to use PBI's CertiDeath product, PBI's business clients "upload a file with [PBI], and [PBI] continuously monitor[s] that file and provid[es] [the client] with a weekly [report]. And [PBI] [does] that until [the client] upload[s] a new file to [PBI].").

[479] PBI, *Global MOVEit Transfer Cyberattack*, https://www.pbinfo.com/faq-communication/ (last accessed Oct. 21, 2024).

[480] PBI, *Data Security*, https://www.pbinfo.com/data-security/ (last accessed Oct. 18, 2024).

[481] PBI, *Privacy Principles*, https://www.pbinfo.com/privacy-principles/ (last accessed Oct. 18, 2024) ("PBI's Privacy Principles (the 'Principles') speak to personally identifiable information, including sensitive personally identifiable information, collected, maintained, used, disclosed, or processed in connection with products and services offered by PBI.").

rights[]"[482] and claims: "Data security is a company imperative. PBI strives to protect personally identifiable information that [it] collect[s], maintain[s], process[es], or disclose[s], including by using appropriate administrative, physical, and technical safeguards."[483]

1844. PBI's website specifically recognizes the importance of having systems and processes in place to protect and secure sensitive PII it obtains and/or transfers via the Internet:

> **ONLINE PRIVACY**
>
> PBI strives to protect the privacy of personally identifiable information obtained over the Internet and strives to apply the Principles and evolving standards to the online environment.[484]
>
> **IDENTITY THEFT**
>
> PBI strives to prevent the acquisition of information from our products and services for improper purposes, such as identity theft. PBI believes in the importance of notifying individuals who may have had their sensitive personally identifiable information acquired by an unauthorized individual, as appropriate.[485]

1845. PBI also acknowledges the importance of ensuring that its data security systems and processes are compliant with legal regulations and industry standards:

> **ACCOUNTABILITY**
>
> PBI supports the accountability of information security standards and practices, responsible and effective federal regulation of the data industry, and legislation governing the practices of all data providers. PBI also supports industry oversight and active engagement with the privacy community. PBI believes that strong

[482] PBI, *Privacy Principles*, https://www.pbinfo.com/privacy-principles/ (last accessed Oct. 18, 2024).

[483] PBI, *Privacy Principles*, https://www.pbinfo.com/privacy-principles/ (last accessed Oct. 18, 2024).

[484] PBI, *Privacy Principles*, https://www.pbinfo.com/privacy-principles/ (last accessed Oct. 18, 2024).

[485] PBI, *Privacy Principles*, https://www.pbinfo.com/privacy-principles/ (last accessed Oct. 18, 2024).

> privacy and information security protections are vital for an effective and trusted data industry.[486]
>
> [. . .]
>
> **COMPLIANCE**
>
> PBI will obtain assessments from an independent auditor, who uses procedures and standards generally accepted in the profession to assess PBI's controls relevant to security, availability, and confidentiality, as appropriate.[487]

1846. PBI claims to have "the largest team of data scientists, product developers, security and IT, and subject matter experts in the industry[]"[488] and "aspire[s] to protect individuals' privacy through the design of [its] products and services, by credentialing, monitoring, and auditing [its] business clients as appropriate, and through other information security safeguards."[489]

1847. PBI promises its business clients, including the PBI Bellwether Defendants, that "[p]rotecting and securing [their] information is [PBI's] highest priority."[490]

1848. PBI makes the same promises to consumers: "PBI recognizes the importance of protecting personal information. We use a variety of administrative, physical and technical security measures intended to safeguard your personal information."[491]

---

[486] PBI, *Privacy Principles*, https://www.pbinfo.com/privacy-principles/ (last accessed Oct. 18, 2024).

[487] PBI, *Privacy Principles*, https://www.pbinfo.com/privacy-principles/ (last accessed Oct. 18, 2024).

[488] PBI, We Find the Hardest to Find People – Access to a Team of Experts, https://www.pbinfo.com/ (last accessed Oct. 18, 2024).

[489] PBI, *Privacy Principles*, https://www.pbinfo.com/privacy-principles/ (last accessed Oct. 18, 2024).

[490] PBI, We Find the Hardest to Find People – Confidence Your Data is Secure, https://www.pbinfo.com/ (last accessed Oct. 18, 2024).

[491] PBI, *Privacy Policy*, https://www.pbinfo.com/privacy-policy/ (last accessed Oct. 18, 2024).

1849. According to PBI's website, "PBI uses a multi-layered approach to protect data securely that includes, but is not limited to the following: implementing secure development practices, including annual training for our IT team, real time scanning of code changes for vulnerabilities, web application firewalls, n-tier application architecture, required security awareness training program for all employees at onboarding and on a regular basis, data loss prevention tools to alert and block transfers of sensitive data, and a consolidated SIEM solution that correlates alerts and events across multiple environments.[492]

1850. PBI claims that its "data security team manages this multi-layered security architecture by performing over 30 security reviews of quarterly audit checks to test compliance against security policies."[493]

1851. PBI also claims that its "formalized security program follows industry-recognized security frameworks" and "undergoes an annual SSAE 18 SOC2, Type II audit by an independent third-party[.]"[494] According to PBI's website:

> PBI regularly uses third parties to test and audit our security controls. We conduct monthly and quarterly vulnerability assessments and penetration tests of PBI's internal and external network and application security, and conduct annual application penetration tests.[495]

With respect to "Network Security," PBI's website states:

> PBI's network incorporates several layers of protection to harden both corporate and production environments including 24/7 monitoring and alerts for critical events and failures, disabling unnecessary connections and services, regular OS and software patching, next generation firewalls with intrusion prevention and intrusion detection software, anti-virus scanning, and dedicated security event management system with 24/7 alerting.

---

[492] PBI, *Data Security*, https://www.pbinfo.com/data-security/ (last accessed Oct. 18, 2024).

[493] PBI, *Data Security*, https://www.pbinfo.com/data-security/ (last accessed Oct. 18, 2024).

[494] PBI, We Find the Hardest to Find People – Confidence Your Data is Secure, https://www.pbinfo.com/ (last accessed Oct. 18, 2024).

[495] PBI, *Data Security*, https://www.pbinfo.com/data-security/ (last accessed Oct. 18, 2024).

> PBI implements the security principle of least privilege access. Access to client information and PBI technology is based upon PBI employees job function, restricted by a valid need-to-know basis, and only used as is necessary to provide the authorized services. Additional access controls include multi-factor authentication and intrusion detection protection program. User accounts and permissions are audited on a quarterly basis.
>
> Data in-transit across our network and data at-rest stored in our databases are encrypted using advanced encryption standards. The security of our databases is tested on a quarterly basis.[496]

1852. According to its website, PBI "provides products and services . . . that help reduce and prevent fraud, mitigate risk, and fulfill fiduciary responsibilities in ways that protect individual's privacy."[497]

1853. Contrary to these outward assurances, however, PBI failed to adequately secure and safeguard the highly sensitive PII that it solicited and collected from the PBI Bellwether Defendants. PBI did not have adequate data security measures in place to protect and maintain the highly sensitive PII entrusted to it, nor did it ensure its vendors and business associates reasonably and adequately secured, safeguarded, and otherwise protected consumers' PII, which PBI shared with third-party vendors, such as Progress, through PBI's use of the MOVEit Transfer software. Instead, PBI's website wholly fails to disclose the truth: that PBI lacks sufficient processes to protect the PII that is entrusted to it.

D. Genworth Defendants knew they had duties to protect the PBI Bellwether Plaintiffs' and Class Members' PII, and assured them that they would.

1854. In the ordinary course of their business, Genworth Defendants collect highly sensitive PII from customers and potential customers, including demographic information, contact

[496] PBI, *Data Security*, https://www.pbinfo.com/data-security/ (last accessed Oct. 18, 2024).

[497] PBI, *Privacy Principles*, https://www.pbinfo.com/privacy-principles/ (last accessed Oct. 18, 2024).

information (including address, phone number, and email), Social Security numbers, financial and banking information, medical information, and information about customers' beneficiaries.[498]

1855. As a condition of receiving life insurance services through Genworth, PBI Bellwether Plaintiffs and PBI Bellwether Class Members were required to provide their highly sensitive PII to Genworth.

1856. Genworth directs customers and potential customers to use "MyGenworth, [their] secure customer website."[499]

1857. "To access information about [their] existing insurance policies or accounts and for some other purposes, [customers] must register an account. When [they] register, [Genworth] [ ] ask[s] for more personal information. That may include [the customer's] policy or account number, [their] date of birth and [their] [S]ocial [S]ecurity number."[500]

1858. Statements on Genworth's websites indicate that Genworth understands their obligations to protect customers' PII:

> Federal and state laws require that we tell you how we collect, use, share, and protect your personal information. Those laws also limit how we may use your personal information and how we may share it with others. Protecting the privacy and security of your personal information is very important to us.[501]

---

[498] *See "Did You Know*," Genworth, https://www.genworth.com/customer-service (last accessed Nov. 27, 2024).

[499] *Login to Manage Your Genworth Account*, Genworth (May 5, 2023), https://www.genworth.com/login.

[500] *Online Privacy Policy – Personal Information*, Genworth, https://www.genworth.com/online-privacy-policy (last updated April 10, 2024).

[501] *Online Privacy Policy – Scope*, Genworth, https://www.genworth.com/online-privacy-policy (last updated April 10, 2024); *see also Genworth Privacy Notice*, Genworth (Jan. 1, 2018), https://pro.genworth.com/riiproweb/productinfo/pdf/45242.pdf; *Genworth Privacy Notice – Frequently Asked Questions*, Genworth (June 18, 2013), https://pro.genworth.com/riiproweb/productinfo/pdf/106681.pdf; *Genworth HIPAA Privacy Policy (Health Information)*, Genworth (Oct. 30, 2013), https://a-us.storyblok.com/f/1008916/8c37f805f5/157407_103013.pdf; *Genworth Disclosure – Confidentiality for Victims of Domestic Violence*, Genworth (Nov. 3, 2015), https://www.genworth.com/dam/Americas/US/PDFs/Consumer/Confidentiality_Protocol_

1859. Genworth claims that "[w]orking to protect [its customers'] personal information is one of [the] promises that enables [Genworth] to help millions of policyholders secure their financial lives, families, and futures."[502]

1860. Genworth's websites warrant to consumers that:

> Once we receive your information, we use procedures and technologies designed to prevent unauthorized access to your personal information and to protect against the loss, misuse, and alteration of information under our control. We maintain physical, electronic, and procedural protections to protect personal information in accordance with applicable standards.[503]

Genworth explicitly promises customers:

> We require that service providers who have access to your personal information implement similar standards. We require service providers to agree to keep your personal information confidential. Service providers who violate our privacy terms are subject to having their contract terminated.[504]

1861. Genworth promises customers that Genworth has "implemented technical, physical, and process safeguards to maintain the confidentiality of your information."[505]

1862. Genworth also promises customers:

> We restrict access to personal information to employees and service providers who have a legitimate business need in providing products or services to you. Employees

---

Notice.pdf; *Additional Privacy Information for California Residents*, Genworth, https://www.genworth.com/online-privacy-policy/ccpa (last updated March 27, 2024).

[502] *Fraud & Information Protection*, Genworth (May 4, 2023), https://www.genworth.com/fraud-and-information-protection.

[503] *Online Privacy Policy*, Genworth, https://www.genworth.com/online-privacy-policy.html (last updated April 10, 2024).

[504] *Online Privacy Policy*, Genworth, https://www.genworth.com/online-privacy-policy.html (last updated April 10, 2024).

[505] *USLI Policyholder Fraud/Scam Information*, Genworth (May 18, 2020), https://www.genworth.com/fraud-and-information-protection/policyholder-fraud-information.

> who violate these terms are subject to disciplinary action. Service providers who violate these terms are subject to having their contract terminated.[506]

1863. Genworth provided PBI Bellwether Plaintiffs' and Class Members' PII to PBI by uploading files containing that data to PBI's MOVEit Transfer server via PBI's "MOVEit administrative portal software."[507]

1864. Genworth Defendants understood that the PII they solicited and collected from PBI Bellwether Plaintiffs and Class Members was highly sensitive.

1865. Death records have long been known to be valuable to cybercriminals because they facilitate identity fraud. In November 2011, due to privacy and identity theft concerns, the Social Security Administration redacted and no longer included death data derived from State sources.[508]

1866. Genworth specifically recognizes that "[f]raudsters may read obituaries, learn the family's details, and use this opportunity to take advantage of a grieving spouse. They may ask the spouse to settle the deceased's fake debt."[509]

1867. Accordingly, Genworth recognizes that customers are especially vulnerable to fraud and scams.

---

[506] *Online Privacy Policy – How We Protect Your Personal Information*, Genworth, https://www.genworth.com/online-privacy-policy (last updated Apr. 10, 2024).

[507] PBI, *Global MOVEit Transfer Cyberattack*, https://www.pbinfo.com/faq-communication/ (last accessed Oct. 21, 2024).

[508] *See, e.g.*, Kevin Sack, *Researchers Wring Hands as U.S. Clamps Down on Death Record Access*, The New York Times (Oct. 8, 2012), https://www.nytimes.com/2012/10/09/us/social-security-death-record-limits-hinder-researchers.html (in November 2011, "the Social Security Administration [started] to limit access to its death records amid concerns about identity theft"); Nancy Amons, *Government Still Declares Living Woman Dead*, WSMV News (Feb. 20, 2008), https://web.archive.org/web/20080222151141/http://www.wsmv.com/news/15357541/detail.html.

[509] *The Most Common Financial Scams Taking Advantage of Older Americans*, Genworth (Apr. 11, 2023), https://www.genworth.com/aging-and-you/resources/avoiding-senior-citizen-scams.

1868. On its website, Genworth Financial provides a litany of resources and articles to warn its customers:

> Every year, 5 million older Americans are targeted by financial scammers. [. . .] Why do con artists prey on older people? Because they are easy targets likely to have a nest egg that's ripe for the picking. Additionally, they're more susceptible to scams that promise longer, healthier lives. Finally, they're among the least likely to report the crimes. The lack of reporting may be for a variety of reason[s] including that it can take longer to realize they've been scammed, they may not know how to report it, they may feel embarrassed, or they may worry that their family will think they can no longer manage their financial affairs.[510]

1869. Genworth also knows that the Genworth customer population is especially susceptible to email/phishing scams.[511] Genworth explains that "[s]eniors make twice as many phone purchases as any other demographic group. Telemarketing scams are hard to trace and can often lead to repeat offenders who prey on easy targets."[512] Additionally, "[o]lder people generally aren't as internet savvy as their younger counterparts and may not recognize online scams."[513]

1870. Genworth specifically advises customers to "be careful about the information that [they] share online" because "[c]riminals often seek to commit fraud by piecing together information about the victim's life from social media and other online outlets. This information may allow them to guess passwords, reset [ ] passwords, or create fake online accounts in your name but with their address. Remember that even if you have strong privacy settings on your social

---

[510] *Id.*

[511] *Id.* ("Email/phishing scams: A scammer posing as the IRS, a bank, or another seemingly legitimate organization sends an email to your parents asking them to update or verify their personal information. Alternatively, the scammer may mimic a relative or friend's email address and [ask] for money to be wired for various reasons.").

[512] *Id.*

[513] *Id.*

media content, if one of your connection's accounts is hacked, your information may be accessible to the criminal as well."[514]

1871. The Genworth Defendants understood their obligations to protect the highly sensitive PII they solicited and collected from their customers, but broke their promises to "implement[] technical, physical, and process safeguards to maintain the confidentiality of [their customers'] information."[515]

E. Milliman Defendants knew they had duties to protect the PBI Bellwether Plaintiffs' and Class Members' PII, and assured them that they would.

1872. Milliman collects, stores, and transfers consumers' PII to third-party vendors, including PBI, in connection with the services Milliman provides to clients, which include life and health insurance companies. Milliman relies on PBI's data verification, death audit, and participant location services in the regular course of business.

1873. As explained by an article published on Milliman, Inc.'s website:

> Defined Benefit plans face daily administrative struggles, including growing structural complexity, administrative changes, digital maintenance, possible outdated software, bad plan data, and a host of other challenges. Bad participant addresses and contact information are among the less exciting and hard-to-fix items of plan data, yet without regular maintenance, they could render all other aspects of pension administration irrelevant. It is imperative that defined benefit plans keep good participant address information on file as several notices are required to be mailed out regularly.
>
> * * *
>
> To locate participants, individual address searches can be conducted as returned mail is received using an industry-recognized vendor such as PBI [ ]. When working with a larger population, these vendors may also be able to perform bulk address

[514] *USLI Policyholder Fraud/Scam Information*, Genworth (May 18, 2020), https://www.genworth.com/fraud-and-information-protection/policyholder-fraud-information.

[515] *Fraud & Information Protection*, Genworth (May 4, 2023), https://www.genworth.com/fraud-and-information-protection.

> searches, which typically require a spreadsheet containing participant names, SSNs, and birth dates, (file formats and turnaround times differ by vendor).[516]

1874. Milliman Inc.'s website proclaims that "[d]ata security is one of Milliman's top priorities. It is vital that we provide appropriate security to ensure the services we provide to our clients are of the highest standards."[517]

1875. Milliman's Data Privacy Policy claims that Milliman "take[s] data privacy very seriously."[518] According to Milliman's Data Privacy Policy:

> Milliman [] may share Personal Data with authorized third-party agents or contractors that perform services for Milliman. If Milliman shares Personal Data with a third party, Milliman requires that those third parties agree to process Personal Data based on Milliman's instructions and in compliance with this Privacy Policy. Any transfers of Personal Data are subject to appropriate safeguards that are compliant with jurisdiction-specific privacy laws.[519]

1876. Milliman claims that Milliman "stores Personal Data on a secure server that is password protected and shielded from unauthorized access by a firewall. Milliman has in place security policies that are intended to ensure the security and integrity of all Personal Data. Milliman has appropriate technical and organizational measures in place to protect against unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of, damage to,

---

[516] Kristina Pizano and Haydee Scheel, *Address maintenance – One good address is one less headache*, Milliman (Nov. 17, 2020), https://www.milliman.com/en/insight/address-maintenance-one-good-address-is-one-less-headache.

[517] *Milliman data breach disclosures – PBI/MOVEit data breach*, Milliman, https://www.milliman.com/en/data-breach-disclosure (last accessed Oct. 24, 2024).

[518] *Millman Global Data Privacy Policy*, Milliman (last updated Aug. 2024), https://www.milliman.com/en/privacy-policy ("This Privacy Policy sets out the principles governing Milliman's use and protection of personal information that individuals and clients share with us ('Personal Data') as well as describing the rights of individuals regarding their Personal Data. This Privacy Policy applies to Milliman's data collection and use through its website and through its business operations.").

[519] *Millman Global Data Privacy Policy – Affiliates and Authorized Third-Party Agents*, Milliman (last updated Aug. 2024), https://www.milliman.com/en/privacy-policy.

Personal Data held or processed by Milliman. If Milliman forwards Personal Data to any third party, Milliman requires that those third parties have appropriate technical and organizational measures in place to comply with this Privacy Policy and applicable laws."[520]

1877. The Milliman Defendants market themselves as "experts" in cybersecurity, claiming that they can "quantify the potential financial impacts of cyber risk and can produce cost-benefit analyses and model a variety of possible risk scenarios to find gaps."[521]

1878. On its website, Milliman, Inc. explicitly recognizes that "cyber risk is an ever shifting landscape. New vectors and new attacks pose major challenges to businesses trying to keep data systems and people safe."[522]

1879. Milliman claims that Milliman offers "a next-generation cyber risk solution that incorporates a forward-looking approach to modeling how cyber risks occur and propagate[,] provides organizational decision makers and risk managers with a more accurate understanding of current vulnerabilities[, and] helps identify emerging threat vectors before they cause damage[.]"[523]

F. MLIC knew it had duties to protect the PBI Bellwether Plaintiffs' and Class Members' PII, and assured them that it would.

1880. MLIC's website repeatedly states that it is keenly cognizant of data privacy risks and has adequate procedures and process in place to prevent them, including its statements that:

---

[520] *Millman Global Data Privacy Policy – Security*, Milliman (last updated Aug. 2024), https://www.milliman.com/en/privacy-policy.

[521] *Risk Solutions – Cyber risk*, Milliman, https://www.milliman.com/en/risk/cyber-risk (last accessed Nov. 27, 2024).

[522] Milliman, Inc., "CRisALIS for cyber" (video), https://www.milliman.com/en/products/complexriskanalysis (last accessed Aug. 9, 2023).

[523] *Complex Risk - Milliman Complex Risk Analysis (CRisALIS)*, Milliman, https://www.milliman.com/en/products/complexriskanalysis (last accessed Nov. 24, 2024).

"We are working with some of the industry's best minds to deploy sophisticated technology such as machine learning, building rapid response solutions that help identify tomorrow's threats, and implementing new approaches to managing risk that actually help people work more efficiently."[524]

"Any organization that deals with sensitive data faces increasing challenges in keeping that data safe. From guarding against sophisticated cyber criminals to preventing accidental data loss, staying safe means keeping one step ahead."[525]

"It is essential for any business to rethink how to best model its cyber risk, with the goal of illuminating blind spots instead of missing them."[526]

"[C]yber risk needs to be analyzed in a way that allows companies to examine the appropriate controls and mitigation techniques, and how causal-based models are a proven way to account for the decisions of both the company and the attacker."[527]

"From guarding against sophisticated cyber criminals to preventing accidental data loss, staying safe means keeping one step ahead."[528]

"Cyber risk is evolving fast. You've got to evolve faster."[529]

---

[524] *Cyber risk – Growing threats demand a smart response*, Milliman, https://www.milliman.com/en/insurance/cyber (last accessed Nov. 27, 2024).

[525] *Cyber risk – Growing threats demand a smart response*, Milliman, https://us.milliman.com/en/risk/cyber (last accessed Nov. 27, 2024).

[526] Chris Harner, et al., *Know your cyber blind spots: The importance of modeling cyber risk for businesses* (March 19, 2021), https://www.milliman.com/en/insight/Know-your-cyber-blind-spots.

[527] Chris Beck, et al., *Does it ever make sense for firms to pay ransomware criminals?* (July 21, 2021), https://www.milliman.com/en/insight/does-it-ever-make-sense-for-firms-to-pay-ransomware-criminals.

[528] *Cyber risk – Growing threats demand a smart response*, Milliman, https://us.milliman.com/en/risk/cyber (last accessed Nov. 27, 2024).

[529] *Cyber risk – Growing threats demand a smart response*, Milliman, https://www.milliman.com/en/insurance/cyber (last accessed Nov. 27, 2024).

1881. MLIC provided PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII to the Milliman Defendants, which then provided that PII to PBI by uploading files containing that data to PBI's MOVEit Transfer server via PBI's "MOVEit administrative portal software."[530]

G. TIAA knew it had duties to protect the PBI Bellwether Plaintiffs' and Class Members' PII, and assured them that it would.

1882. In the ordinary course of its business, TIAA collects sensitive PII from consumers, including: names, gender, dates of birth, Social Security numbers, and addresses.

1883. In the course of collecting PII from its clients, TIAA promises to provide confidentiality and adequate security for client data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

1884. TIAA's Privacy Notice provides that:

> TIAA protects the personal information you provide against unauthorized access, disclosure, alteration, destruction, loss, or misuse. Your personal information is protected by physical, electronic, and procedural safeguards in accordance with federal and state standards. These safeguards include appropriate procedures for access and use of electronic data, provisions for the secure transmission of sensitive personal information on our website, and telephone system authentication procedures. Additionally, we limit access to your personal information to those TIAA employees and agents who need access in order to offer and provide products or services to you. We also require our service providers to protect your personal information by utilizing the privacy and security safeguards required by law.[531]

1885. TIAA provided PBI Bellwether Plaintiffs' and Class Members' PII to PBI by uploading files containing that data to PBI's MOVEit Transfer server via PBI's "MOVEit administrative portal software."[532]

---

[530] PBI, *Global MOVEit Transfer Cyberattack*, https://www.pbinfo.com/faq-communication/ (last accessed Oct. 21, 2024).

[531] *TIAA privacy notice*, TIAA, https://www.tiaa.org/public/support/privacy/privacy-notice (last updated Jan. 2024).

[532] PBI, *Global MOVEit Transfer Cyberattack*, https://www.pbinfo.com/faq-communication/ (last accessed Oct. 21, 2024).

H. Contrary to their statements touting their data security, PBI Bellwether Defendants failed to safeguard PBI Bellwether Plaintiffs' and Class Members' PII.

1886. Contrary to their statements alleged above—touting the security of their systems and promising to safeguard sensitive information in their possession and/or control—PBI Bellwether Defendants failed to adequately secure and safeguard PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII and, instead, allowed it to be compromised in the Data Breach.

1887. Specifically, PBI-Contracting Defendants sent PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' sensitive PII to PBI without assuring that it would remain safe, which was inconsistent with their statements to the public that it would. As evidenced by the occurrence of the Data Breach, PBI lacked adequate processes and policies to safeguard the PII in its possession—which had been provided by PBI-Contracting Defendants. All PBI Bellwether Defendants knew or should have known that information stored on PBI's servers was vulnerable to cyberattack and likely to be compromised.

1. PBI Failed to Secure PBI Plaintiffs' and PBI Class Members' PII and, instead, allowed it to be compromised in the Data Breach

1888. Because of the large volume of sensitive data it collects, stores, and maintains on behalf of its business clients, PBI is "a prime target for a group like the Cl0p ransomware gang."[533]

1889. PBI "became aware of the MOVEit [Data Breach] on June 2, 2023[,]"[534] after Progress "publicly disclosed zero-day vulnerabilities that impacted its MOVEit Transfer software."[535]

---

[533] *What happened in the PBI data breach?*, Cloaked (June 20, 2024), https://www.cloaked.com/post/pbi-data-breach.

[534] PBI, *Global MOVEit Transfer Cyberattack*, https://www.pbinfo.com/faq-communication/ (last accessed Oct. 21, 2024).

[535] *Data Breach Notifications – Pension Benefit Information, LLC*, Office of the Maine Attorney General (July 11, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-

1890. PBI "launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the potential impact of the vulnerabilities' presence on its MOVEit Transfer servers and on the data housed on the servers."[536]

1891. PBI's "investigation determined that a threat actor exploiting a zero-day vulnerability, accessed one of PBI's MOVEit Transfer servers on May 29th, 2023, and May 30th, 2023, and exfiltrated certain data from that MOVEit Transfer server during that time. PBI subsequently undertook a time-consuming and detailed review of the data stored on the server at the time of the event to understand the contents of that data and to which business clients that data relates."[537]

1892. PBI determined that the Data Breach "impact[ed] a small percentage of [its] clients who use the MOVEit administrative portal software resulting in access to private records."[538]

1893. According to PBI, Cl0p "did not gain access to PBI's other systems – access was only gained to the MOVEit administrative portal subject to the vulnerability."[539]

---

a1252b4f8318/14efac97-4a7c-4322-98eb-2e953884eb58/f135d329-507c-484c-9798-b46d470c5d96/Notice%20of%20Data%20Event%20-%20PBI%20-%20ME.pdf.

[536] *Data Breach Notifications – Pension Benefit Information, LLC*, Office of the Maine Attorney General (July 11, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/14efac97-4a7c-4322-98eb-2e953884eb58/f135d329-507c-484c-9798-b46d470c5d96/Notice%20of%20Data%20Event%20-%20PBI%20-%20ME.pdf.

[537] *Data Breach Notifications – Pension Benefit Information, LLC*, Office of the Maine Attorney General (July 11, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/14efac97-4a7c-4322-98eb-2e953884eb58/f135d329-507c-484c-9798-b46d470c5d96/Notice%20of%20Data%20Event%20-%20PBI%20-%20ME.pdf.

[538] PBI, *Global MOVEit Transfer Cyberattack*, https://www.pbinfo.com/faq-communication/ (last accessed Oct. 21, 2024).

[539] Bill Toulas, *MOVEit breach impacts Genworth, CalPERS as data for 3.2 million exposed*, BleepingComputer (updated June 24, 2023), https://www.bleepingcomputer.com/news/security/moveit-breach-impacts-genworth-calpers-as-data-for-32-million-exposed/.

1894. PBI maintains that the Data Breach did not result in "access to PBI's core systems or software[,]"[540] and only affected PBI clients whose data was transferred using PBI's MOVEit Transfer administrative portal.[541]

1895. The PBI MOVEit Transfer server that was targeted in the Data Breach was located within PBI's network environment and stored PII provided to PBI by the PBI Bellwether Defendants, including the PII of the PBI Bellwether Plaintiffs and PBI Bellwether Class Members.

1896. PBI claims that it "promptly patched its instance of MOVEit, assembled a team of cybersecurity and privacy specialists, notified federal law enforcement, and contacted impacted clients."[542]

1897. On or about June 4, 2023, "PBI began to provide notice of [the Data Breach] to potentially affected business clients with an offer to provide notification services to potentially impacted individuals on their behalf and at their direction."[543]

1898. PBI "conducted a manual review of [its] records to confirm the identities of individuals potentially affected by [the Data Breach] and their contact information to provide notifications."[544]

---

[540] PBI, *Global MOVEit Transfer Cyberattack*, https://www.pbinfo.com/faq-communication/ (last accessed Oct. 21, 2024).

[541] *What happened in the PBI data breach?*, Cloaked (June 20, 2024), https://www.cloaked.com/post/pbi-data-breach.

[542] PBI, *Global MOVEit Transfer Cyberattack*, https://www.pbinfo.com/faq-communication/ (last accessed Oct. 21, 2024).

[543] *Data Breach Notifications – Pension Benefit Information, LLC*, Office of the Maine Attorney General (July 11, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/14efac97-4a7c-4322-98eb-2e953884eb58/f135d329-507c-484c-9798-b46d470c5d96/Notice%20of%20Data%20Event%20-%20PBI%20-%20ME.pdf.

[544] *Data Breach Notifications – Pension Benefit Information, LLC*, Office of the Maine Attorney General (July 11, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-

1899. In notice letters sent to individual consumers on behalf of PBI's business clients, including the PBI-Contracting Defendants, PBI "encourage[d] [impacted individuals] to remain vigilant against incidents of identity theft and fraud by reviewing [their] account statements and monitoring [their] free credit reports for suspicious activity and to detect errors."[545]

1900. Following the Data Breach, PBI assured its business clients that they could "continue to safely do business with PBI," because "PBI systems were not impacted, outside of the isolated MOVEit Transfer server."[546] PBI also told its business clients: "If you are hesitant to use MOVEit software at this time, we have other data transfer options or layers of optional security that can be added to further secure your data."[547] Despite these assurances, some of PBI's business clients elected to stop transmitting their customers' PII to PBI via MOVEit.[548]

---

a1252b4f8318/14efac97-4a7c-4322-98eb-2e953884eb58/f135d329-507c-484c-9798-b46d470c5d96/Notice%20of%20Data%20Event%20-%20PBI%20-%20ME.pdf.

[545] *Data Breach Notifications – Pension Benefit Information, LLC*, Office of the Maine Attorney General (July 11, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/14efac97-4a7c-4322-98eb-2e953884eb58/f135d329-507c-484c-9798-b46d470c5d96/Notice%20of%20Data%20Event%20-%20PBI%20-%20ME.pdf.

[546] PBI, *Global MOVEit Transfer Cyberattack*, https://www.pbinfo.com/faq-communication/ (last accessed Oct. 21, 2024).

[547] PBI, *Global MOVEit Transfer Cyberattack*, https://www.pbinfo.com/faq-communication/ (last accessed Oct. 21, 2024).

[548] *See, e.g.*, *PBI Data Security Incident*, Tennessee Consolidated Retirement System (July 10, 2023), https://treasury.tn.gov/Portals/0/Documents/Retirement/PBIIncidentFAQ.pdf ("[The Tennessee Consolidated Retirement System ('TCRS')] uses PBI to help identify member deaths and prevent overpayments. [. . .]. MOVEit Transfer is a managed file transfer software, utilized by PBI to receive data from companies like TCRS. [. . .]. TCRS has not transmitted any information via MOVEit since May 2023."); *Letter to the Office of the Maine Attorney General*, Milliman (August 14, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/903ecb46-93b2-4986-aae5-ec7e088625f8/31ce7f5a-a49a-48eb-a52b-33dd1d68bc1a/23.08.14%20ME%20AG%20Notification%20Letter.pdf ("Milliman has stopped transferring data to PBI pending further evaluation of PBI's information security practices.").

2. Genworth Defendants Failed to Secure PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' Sensitive PII and, instead, allowed it to be compromised in the Data Breach

1901. PBI waited until June 16, 2023—two weeks after it first learned of the Data Breach—to inform Genworth "that specific Genworth files containing policyholder and agent information were compromised [in the Data Breach]."[549]

1902. Genworth Defendants waited over two weeks before they informed impacted individuals—such as PBI Bellwether Plaintiffs and Class Members—that their sensitive PII was involved in the Data Breach.[550]

1903. Genworth reported that "the personal information of a significant number of insurance policyholders or other customers of its life insurance businesses was unlawfully accessed [in the Data Breach][.]"[551]

1904. Genworth's investigation subsequently confirmed that the PII of approximately 2.5 to 2.7 million Genworth customers and insurance agents was accessed and acquired by Cl0p in the Data Breach.[552]

---

[549] *MOVEit Security Event*, Genworth (last updated Aug. 31, 2023), https://www.genworth.com/moveit#backgroundinfo.

[550] *MOVEit Security Event*, https://www.genworth.com/moveit (Aug. 9, 2023 update).

[551] Genworth Financial, Inc. SEC Current Report (Form 8-K) (June 16, 2023), https://www.sec.gov/Archives/edgar/data/1276520/000119312523172549/d463993d8k.htm.

[552] *MOVEit Security Event – Who Was Affected*, Genworth (last updated Aug. 31, 2023), https://www.genworth.com/moveit#whoaffected (confirming that the PII of "a very significant portion of [Genworth's] customers across long-term care insurance, life insurance, and annuities" was exposed in the Data Breach); *see also* Bill Toulas, *MOVEit breach impacts Genworth, CalPERS as data for 3.2 million exposed*, BleepingComputer (June 23, 2023), https://www.bleepingcomputer.com/news/security/moveit-breach-impacts-genworth-calpers-as-data-for-32-million-exposed/; Zach Simas, *Unpacking the MOVEit Breach: Statistics and Analysis*, Emsisoft (last updated June 28, 2024), https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/.

1905. Genworth customers and insurance agents whose PII was exposed in the Data Breach were sent written data breach notice letters from both PBI and Genworth.[553] The PBI letters offered impacted individuals 24 months of free credit monitoring and identity restoration services.[554]

1906. According to Genworth, "PBI [] mail[ed] notification letters [to impacted Genworth customers and insurance agents] in batches through the month of August [2023][.]"[555]

1907. For Genworth customers, the PII compromised in the Data Breach includes: full names, dates of birth, Social Security numbers, states of residence, zip codes, policy numbers, the role of the individual (e.g., Annuitant, Joint Insured, Owner, etc.), and general product type. If deceased, the exposed PII also includes the city and date of death, along with the source of that information.[556]

1908. For Genworth insurance agents, the PII compromised in the Data Breach includes: full names, dates of birth, Social Security numbers, full addresses, and preferred full addresses. If deceased, the exposed PII also includes date of death and the source of that information.[557]

---

[553] *MOVEit Security Event – Background Information*, Genworth (last updated Aug. 31, 2023), https://www.genworth.com/moveit#backgroundinfo.

[554] *MOVEit Security Event – Background Information*, Genworth (last updated Aug. 31, 2023), https://www.genworth.com/moveit#backgroundinfo; *see also Template Letter for Impacted Living Massachusetts Residents*, PBI, https://a-us.storyblok.com/f/1008916/b7006ed03d/pbi-consumer-notice-ma.pdf (last accessed Oct. 26, 2024); *Template Letter for All States Except for Massachusetts for Impacted Living Individuals*, PBI, https://a-us.storyblok.com/f/1008916/4f74990acf/pbi-consumer-notice.pdf (last accessed Oct. 26, 2024).

[555] *MOVEit Security Event – Background Information*, Genworth (last updated Aug. 31, 2023), https://www.genworth.com/moveit#backgroundinfo.

[556] *MOVEit Security Event – Who Was Affected*, Genworth (last updated Aug. 31, 2023), https://www.genworth.com/moveit#whoaffected.

[557] *MOVEit Security Event – Who Was Affected*, Genworth (last updated Aug. 31, 2023), https://www.genworth.com/moveit#whoaffected.

1909. Genworth warned customers that the PII of their deceased family members who "had a policy/contract with Genworth, but passed away recently . . . may [also] have been affected by the [Data Breach]."[558] Genworth urged those customers to review information contained in PBI's data breach notice letters "to protect the estate of your family member from identity fraud."[559]

1910. Following the Data Breach, Genworth assured customers that Genworth had "implemented technical, physical, and process safeguards to maintain the confidentiality of [its] customer information. Further, [Genworth] require[s] third parties that receive and store the personal information of our customers to take similar steps, and [] work[s] to understand the measures they have taken."[560] Genworth further promised to "focus on and seek opportunities to improve how third parties protect the data of [its] customers."[561]

1911. Genworth maintains that "none of its information systems or business operations were impacted as a result of [the Data Breach]."[562]

---

[558] *MOVEit Security Event – Who Was Affected*, Genworth (last updated Aug. 31, 2023), https://www.genworth.com/moveit#whoaffected.

[559] *MOVEit Security Event – Who Was Affected*, Genworth (last updated Aug. 31, 2023), https://www.genworth.com/moveit#whoaffected; *see also Template Letter for Impacted Deceased Massachusetts Residents*, PBI, https://a-us.storyblok.com/f/1008916/af4e6e8c42/pbi-consumer-notice-ma-deceased.pdf (last accessed Oct. 26, 2024); *Template Letter for All States Except for Massachusetts for Impacted Deceased Individuals*, PBI, https://a-us.storyblok.com/f/1008916/746b913da7/pbi-consumer-notice-deceased.pdf (last accessed Oct. 26, 2024).

[560] *MOVEit Security Event – Background Information*, Genworth (last updated Aug. 31, 2023), https://www.genworth.com/moveit#backgroundinfo.

[561] MOVEit Security Event – Background Information, Genworth (last updated Aug. 31, 2023), https://www.genworth.com/moveit#backgroundinfo.

[562] *MOVEit Security Event – Background Information*, Genworth (last updated Aug. 31, 2023), https://www.genworth.com/moveit#backgroundinfo ("Genworth does not use the MOVEit (or similarly impacted GoAnywhere) software applications *on any company system*.") (emphasis added).

3. Milliman Defendants and MLIC Failed to Secure PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' Sensitive PII and, instead, allowed it to be compromised in the Data Breach

1912. PBI waited until June 16, 2023—two weeks after it first learned of the Data Breach—to inform Milliman "that PBI experienced a data security incident affecting the data of [Milliman's] clients."[563]

1913. Milliman reported to the Maine Attorney General as follows:

> Milliman Solutions provides risk assessment services to clients including life insurance companies. As part of those services, Milliman Solutions utilizes a third-party vendor, Pension Benefit Information, LLC ("PBI"), to conduct research on whether consumers have passed away. For that purpose, Milliman Solutions transferred data regarding its clients' consumers to PBI utilizing a secure and encrypted file transfer protocol. PBI recently notified Milliman Solutions that PBI experienced a data security incident affecting the data of Milliman Solutions' clients. Specifically, PBI disclosed that it utilized the "MOVEit Transfer" software provided by Progress Software Corporation ("Progress Software") for PBI's secure file transfer protocol ("SFTP") servers. PBI also indicated that it stored Milliman Solutions' clients' data on PBI's SFTP servers utilizing the MOVEit Transfer software.
>
> * * *
>
> PBI explained it [ ] conducted a manual review of its data to confirm the identities of individuals potentially affected by this event. PBI completed that review on June 16, 2023, and confirmed to Milliman Solutions at that time that the personal information of certain consumers of Milliman Solutions' clients were affected and Milliman Solutions, following reconciliation of the data, was able to recently inform its clients of the scope of individuals whose information may have been affected. The Milliman Solutions clients whose consumer data was affected by the incident include [MLIC] [564]

---

[563] *Data Breach Notifications – Milliman Solutions LLC*, Office of the Maine Attorney General (July 17, 2023), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a98d9ae9-b898-4aaa-8dde-de04551aaedb.shtml; *see also* Milliman, *Data Breach Notice* (July 17, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/a98d9ae9-b898-4aaa-8dde-de04551aaedb/af45f431-a61c-4c76-9d70-f31ab3236aa7/PBI%20-%20Sample%20Notification%20Letter.pdf.

[564] *Data Breach Notifications – Milliman Solutions LLC*, Office of the Maine Attorney General (June 16, 2023), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a98d9ae9-b898-4aaa-8dde-de04551aaedb.shtml.

1914. Although PBI's "manual review of its data to confirm the identities of individuals potentially affected" and Milliman's subsequent "reconciliation of the data" was reportedly completed on June 16, 2023,[565] PBI and Milliman waited another month to begin notifying individual consumers of the Data Breach on July 17, 2023.[566]

1915. Milliman Defendants' submission to the Maine Attorney General explains that they possessed PII of PBI Bellwether Plaintiffs and PBI Bellwether Class Members provided by MLIC to Milliman Defendants, and transferred that PII to PBI, which was then subject to (and compromised in) the Data Breach.

1916. Milliman provided additional updates to the Office of the Maine Attorney General on August 14, 2023[567] and January 12, 2024.[568]

1917. According to Milliman's August 14, 2023 letter to the Office of the Maine Attorney General, PBI completed an additional "review on July 21, 2023, and confirmed to Milliman at that time that the personal information of certain [additional] consumers of Milliman's clients were

---

[565] *Data Breach Notifications – Milliman Solutions LLC*, Office of the Maine Attorney General (June 16, 2023), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a98d9ae9-b898-4aaa-8dde-de04551aaedb.shtml.

[566] *See Data Breach Notifications – Milliman Solutions LLC*, Office of the Maine Attorney General (June 16, 2023), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a98d9ae9-b898-4aaa-8dde-de04551aaedb.shtml (noting "Date(s) of consumer notification: **Starting 07/17/2023**) (emphasis in original); *see also PBI Sample Notification Letter*, Milliman (July 17, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/a98d9ae9-b898-4aaa-8dde-de04551aaedb/af45f431-a61c-4c76-9d70-f31ab3236aa7/PBI%20-%20Sample%20Notification%20Letter.pdf.

[567] *Data Breach Notifications – Milliman Solutions LLC*, Office of the Maine Attorney General (August 14, 2023), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/903ecb46-93b2-4986-aae5-ec7e088625f8.shtml.

[568] *Data Breach Notifications – Milliman Solutions LLC*, Office of the Maine Attorney General, (January 12, 2024), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/05d64329-7db7-4ece-baaa-3f98583b4eb6.shtml.

affected and Milliman, following reconciliation of the data, was able to recently inform its clients of the scope of individuals whose information may have been affected."[569]

1918. In the same August 14, 2023 letter, Milliman reported that:

> PBI has advised [Milliman] that it immediately took steps to patch the vulnerability in its MOVEit Transfer software, and PBI is reviewing and enhancing its information security policies and procedures.
>
> Milliman has stopped transferring data to PBI pending further evaluation of PBI's information security practices. Milliman is also evaluating potential vendor management and security enhancements."[570]

1919. According to Milliman's January 12, 2024 letter to the Office of the Maine Attorney General, "[s]ince [its] initial August 14, 2023 notice, Milliman further assessed PBI's notification and, as a result, issued additional notifications, including for deceased individuals[.]"[571]

1920. Milliman clients' customers whose PII was exposed in the Data Breach—including, but not limited to, MLIC's customers—were sent written data breach notice letters from PBI.[572]

---

[569] *Letter to the Office of the Maine Attorney General*, Milliman (August 14, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/903ecb46-93b2-4986-aae5-ec7e088625f8/31ce7f5a-a49a-48eb-a52b-33dd1d68bc1a/23.08.14%20ME%20AG%20Notification%20Letter.pdf.

[570] *Letter to the Office of the Maine Attorney General*, Milliman (August 14, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/903ecb46-93b2-4986-aae5-ec7e088625f8/31ce7f5a-a49a-48eb-a52b-33dd1d68bc1a/23.08.14%20ME%20AG%20Notification%20Letter.pdf.

[571] *Data Breach Notifications – Milliman Solutions LLC*, Office of the Maine Attorney General (January 12, 2024), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/05d64329-7db7-4ece-baaa-3f98583b4eb6.shtml; *see also Letter to the Office of the Maine Attorney General*, Milliman (January 12, 2024), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/05d64329-7db7-4ece-baaa-3f98583b4eb6/b0258551-c4d0-4e10-9938-b3c24dccec18/24.01.12%20Notification%20Letter.pdf.

[572] *See, e.g.*, *PBI Sample Notification Letter*, Milliman (July 17, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/a98d9ae9-b898-4aaa-8dde-de04551aaedb/af45f431-a61c-4c76-9d70-f31ab3236aa7/PBI%20-%20Sample%20Notification%20Letter.pdf.; *Letter to the Office of the Maine Attorney General*, Milliman (August 14, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/903ecb46-93b2-4986-aae5-ec7e088625f8/31ce7f5a-a49a-48eb-a52b-33dd1d68bc1a/23.08.14%20ME%

The PBI letters offered impacted individuals 12 or 24 months of free credit monitoring and identity restoration services.[573]

1921. For Milliman clients' customers, the PII compromised in the Data Breach includes: names, Social Security numbers, dates of birth, and mailing addresses.[574]

1922. At least 1.3 million Milliman clients' customers were impacted in the Data Breach.[575]

4. TIAA Failed to Secure PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' Sensitive PII and, instead, allowed it to be compromised in the Data Breach

1923. PBI waited until June 19, 2023—more than two weeks after it first learned of the Data Breach—to confirm "that certain named TIAA files had been exfiltrated"[576] from PBI's MOVEit Transfer server in the Data Breach.

1924. TIAA reported to the Maine Attorney General as follows:

20AG%20Notification%20Letter.pdf ("PBI is providing written notification to those individuals on behalf of Milliman and its clients identified herein, which includes an offer for 24 months of cost-free credit monitoring. This notification will be sent to the impacted Maine residents via regular mail starting on August 14, 2023.").

[573] *See Letter to the Office of the Maine Attorney General*, Milliman (August 14, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/903ecb46-93b2-4986-aae5-ec7e088625f8/31ce7f5a-a49a-48eb-a52b-33dd1d68bc1a/23.08.14%20ME%20AG%20Notification%20Letter.pdf.

[574] *See Letter to the Office of the Maine Attorney General*, Milliman (August 14, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/903ecb46-93b2-4986-aae5-ec7e088625f8/31ce7f5a-a49a-48eb-a52b-33dd1d68bc1a/23.08.14%20ME%20AG%20Notification%20Letter.pdf.

[575] Zach Simas, *Unpacking the MOVEit Breach: Statistics and Analysis*, Emsisoft (last updated June 28, 2024), https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/.

[576] *Notice of Data Security Incident*, TIAA (July 21, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/ed67df63-aced-4ecb-91ce-602c7e34c83a/573351f0-74fc-4e19-9a62-a51fb837a3bb/Regulator%20Notice%20-%20TIAA%20ME%20AG.pdf.

> TIAA utilizes Pension Benefit Information, LLC ("PBI") to assist with death claim and beneficiary processes. On June 9, 2023, TIAA learned from PBI that it was investigating whether PBI was impacted by the MOVEit Transfer software vulnerability announced by its owner, Progress Software, that could have exposed data to an unauthorized third-party. TIAA worked with PBI to promptly investigate the nature and scope of the event on TIAA participants. On June 19, 2023, PBI confirmed that there were indications that certain named TIAA files had been exfiltrated. TIAA then reconciled such files against [its] records and finished the analysis to determine which participants were impacted by the event; this analysis concluded on June 28, 2023.[577]

According to TIAA, PBI did not begin sending data breach notice letters to affected TIAA participants until July 14, 2023, and the letters were sent "on a rolling basis over the [following] three weeks[.]"[578]

1925. TIAA's participants whose PII was exposed in the Data Breach were sent written data breach notice letters from PBI.[579] The PBI letters offered impacted individuals 24 months of free credit monitoring, fraud consulting and identity restoration services.[580]

---

[577] *Notice of Data Security Incident*, TIAA (July 21, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/ed67df63-aced-4ecb-91ce-602c7e34c83a/573351f0-74fc-4e19-9a62-a51fb837a3bb/Regulator%20Notice%20-%20TIAA%20ME%20AG.pdf.

[578] *Notice of Data Security Incident*, TIAA (July 21, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/ed67df63-aced-4ecb-91ce-602c7e34c83a/573351f0-74fc-4e19-9a62-a51fb837a3bb/Regulator%20Notice%20-%20TIAA%20ME%20AG.pdf.

[579] *Notice of Data Security Incident*, TIAA (July 21, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/ed67df63-aced-4ecb-91ce-602c7e34c83a/573351f0-74fc-4e19-9a62-a51fb837a3bb/Regulator%20Notice%20-%20TIAA%20ME%20AG.pdf ("PBI also agreed to notify TIAA affected individuals through its vendor, Kroll, identifying itself as a TIAA vendor.").

[580] *Notice of Data Security Incident*, TIAA (July 21, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/ed67df63-aced-4ecb-91ce-602c7e34c83a/573351f0-74fc-4e19-9a62-a51fb837a3bb/Regulator%20Notice%20-%20TIAA%20ME%20AG.pdf.

1926. For TIAA participants, the PII compromised in the Data Breach includes: names, Social Security numbers, dates of birth, addresses, and gender."[581]

1927. More than 2.6 million TIAA participants were affected by the Data Breach.[582]

II. PBI Bellwether Defendants Knew the Risks of Data Breaches and Had Duties to Safeguard PBI Bellwether Plaintiffs' and Class Members' PII, but Failed to do so

A. PBI Bellwether Defendants knew they needed to protect the PBI Bellwether Plaintiffs' highly sensitive PII.

1928. PBI Bellwether Defendants were at all times fully aware of their obligations to protect the PII of their customers and policyholders, including the PBI Bellwether Plaintiffs and PBI Bellwether Class Members.

1929. PBI was at all times fully aware of its obligations to protect the highly sensitive consumer data that was entrusted to it by the PBI-Contracting Defendants.

1930. PBI Bellwether Defendants were also aware of the significant repercussions that would result from their failure to protect the highly sensitive consumer data entrusted to them.

1931. By obtaining, collecting, using, and deriving a benefit from the PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII, PBI Bellwether Defendants assumed legal and equitable duties and knew or should have known they were responsible for protecting the PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII from unauthorized access and disclosure.

---

[581] *Notice of Data Security Incident*, TIAA (July 21, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/ed67df63-aced-4ecb-91ce-602c7e34c83a/573351f0-74fc-4e19-9a62-a51fb837a3bb/Regulator%20Notice%20-%20TIAA%20ME%20AG.pdf.

[582] *Teachers Insurance and Annuity Association of America notifying 2,630,717 after PBI alerts them to MOVEit breach*, Dissent (July 22, 2023), https://databreaches.net/2023/07/22/teachers-insurance-and-annuity-association-of-america-notifying-2630717-after-pbi-alerts-them-to-moveit-breach/.

1932. As a regular and necessary part of their businesses, PBI-Contracting Defendants solicit and collect the highly sensitive PII of their customers and/or policyholders, such as PBI Bellwether Plaintiffs and PBI Bellwether Class Members.

1933. Due to the nature of PBI Bellwether Defendants' businesses, they would be unable to engage in their regular business activities without collecting and aggregating PII they know and understand to be sensitive and confidential, such as PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII.

1934. The PBI Bellwether Plaintiffs and PBI Bellwether Class Members relied on the PBI Bellwether Defendants to implement and maintain adequate data security policies and protocols (including vetting, auditing, and monitoring vendors and software companies on which they relied) to keep their PII confidential and securely maintained, to use such PII (if at all) solely for business purposes, and to prevent unauthorized access and disclosure of their PII to unauthorized persons.

1935. The PBI Bellwether Plaintiffs and PBI Bellwether Class Members reasonably expected the PBI Bellwether Defendants would safeguard their highly sensitive information and keep that PII confidential.

1. PBI Bellwether Defendants knew the risks of transferring and storing sensitive information, including the risk of data breaches

1936. Because of the highly sensitive and personal nature of the information PBI Bellwether Defendants transfer, solicit, acquire, store, and/or maintain with respect to customers, policyholders and/or users (referred to collectively herein as "consumers") and other individuals, PBI Bellwether Defendants promise to, among other things: keep PII private; comply with industry standards related to data security and PII, including FTC guidelines; inform consumers of their legal duties and comply with all federal and state laws protecting consumer PII; only use and release PII for reasons that relate to the products and services the PBI Bellwether Plaintiffs and

PBI Bellwether Class Members obtain from the PBI Bellwether Defendants; and provide adequate notice to individuals if their PII is disclosed without authorization.

1937. As sophisticated business entities handling highly sensitive and confidential consumer data, PBI Bellwether Defendants' data security obligations were particularly important, especially in light of the substantial increase in cyberattacks and data breaches in industries handling significant amounts of PII preceding the date of the MOVEit Data Breach.

1938. At all relevant times, PBI Bellwether Defendants knew or should have known that the PBI Bellwether Plaintiffs' and Class Members' PII was a target for malicious actors. Despite such knowledge, PBI Bellwether Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect the PBI Bellwether Plaintiffs' and Class Members' PII from cyberattacks, including, but not limited to, adequately vetting, auditing, monitoring, testing, and patching the software applications they used to store, transfer, and/or otherwise control such PII.

1939. The PBI Bellwether Defendants also knew, or should have known, that the PBI Bellwether Plaintiffs' and Class Members' PII was a target for malicious actors such as C10p.

1940. Despite such knowledge, PBI Bellwether Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect the PBI Bellwether Plaintiffs' and Class Members' PII from cyberattacks, including, but not limited to, adequately vetting, auditing, and monitoring the third-party vendors they used to validate, update, store, and transfer such data (including PBI itself), and adequately vetting, auditing, and monitoring the software applications they used to transfer and receive such data.

1941. In light of recent high profile data breaches—including breaches arising from previously exploited vulnerabilities in other file transfer applications (e.g., Accellion FTA, Fortra

GoAnywhere MFT)—PBI Bellwether Defendants knew or should have known that their electronic records and consumers' PII would be targeted by cybercriminals and ransomware attack groups.

1942. Indeed, PBI Bellwether Defendants knew or should have known that "[t]hird-party software security risks are on the rise, and so are the significant cyber attacks they facilitate. According to a CrowdStrike report, 45% of surveyed organizations said they experienced at least on software supply chain attack in 2021."[583]

1943. Cyberattacks and data breaches of financial services companies or companies storing financial data are also especially problematic because of the potentially permanent disruption they cause to the daily lives of their customers. Stories of identity theft and fraud abound, with hundreds of millions of dollars lost by everyday consumers every year as a result of internet-based identity theft attacks.[584]

1944. The U.S. Government Accountability Office found that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[585]

1945. As highly sophisticated parties that handle sensitive PII, PBI Bellwether Defendants failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of the PBI Bellwether Plaintiffs' and Class Members' PII.

---

[583] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard (last updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software.

[584] Albert Khoury, *Scam alert: 5 most costly data breaches (plus 5 states most targeted)* (July 27, 2022), https://www.komando.com/security-privacy/most-costly-data-breaches/847800/.

[585] *See* U.S. Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, Report to Congressional Requesters (June 2007), https://www.gao.gov/assets/a262904.html.

1946. The ramifications of PBI Bellwether Defendants' failures to keep the PBI Bellwether Plaintiffs' and Class Members' PII secure are severe and long-lasting. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in part because the data can be sold in small batches to multiple buyers as opposed to in bulk to a single buyer. Thus, the PBI Bellwether Plaintiffs and PBI Bellwether Class Members must vigilantly monitor their financial accounts, and are at an increased risk of fraud and identity theft, for many years into the future.

1947. Thus, PBI Bellwether Defendants knew, or should have known, the importance of safeguarding the PII entrusted to them and of the foreseeable consequences if their systems were breached. PBI Bellwether Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring or from mitigating the consequences of the Data Breach.

2. PBI had an obligation to carefully audit Progress's MOVEit Transfer software and cybersecurity practices

1948. PBI knew, or should have known, the importance of safeguarding the PII entrusted to it by the PBI-Contracting Defendants (including PBI Bellwether Plaintiffs' and Class Members' PII), and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on affected individuals as a result of a data breach.

1949. PBI therefore owed a duty to the PBI Bellwether Plaintiffs and PBI Bellwether Class Members to implement and maintain reasonable and adequate data security measures to secure, protect, and safeguard the PII entrusted to it.

1950. PBI should have used its resources to implement and maintain adequate data security procedures and practices.

1951. At the time of the Data Breach, there were known and available steps PBI could have taken to prevent or mitigate the impact of the cyberattack. For example, PBI should have run a script that would scan for when files were done uploading on PBI's "MOVEit administrative portal," and then moved those files off the MOVEit server and over to a storage location the MOVEit file transfer software could not access. "That way, if the file transfer application is ever compromised by a zero day that allows for arbitrary code execution that code can't access any data."[586]

1952. PBI breached its duties to the PBI Bellwether Plaintiffs and PBI Bellwether Class Members by, among other things, failing to employ adequate vendor screening and vetting, including of Progress and its MOVEit Transfer software.

1953. PBI knew or should have known that Progress (a) employed poorly written, outdated, and insecure code in its MOVEit software; (b) failed to update outdated code; and (c) failed to check for known or newly discovered vulnerabilities.

1954. PBI should have but did not vet Progress or its MOVEit Transfer software, and as a result, failed to prevent or detect the Data Breach.

1955. PBI failed to ensure Progress employed and maintained adequate cybersecurity measures to prevent the Data Breach from occurring.

1956. PBI also had obligations arising under the FTC Act, Gramm-Leach-Bliley Act, industry standards, common law, and its own promises and representations made to the PBI-Contracting Defendants, and to the PBI Bellwether Plaintiffs and PBI Bellwether Class Members to keep their PII confidential and protected from unauthorized access and disclosure.

---

[586] Zach Simas, *Unpacking the MOVEit Breach: Statistics and Analysis*, Emsisoft (last updated June 28, 2024), https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/.

3. PBI-Contracting Defendants had obligations to carefully vet and audit their third-party vendors, including PBI

1957. The PBI-Contracting Defendants knew, or should have known, the importance of safeguarding the PII entrusted to them by the PBI Bellwether Plaintiffs and PBI Bellwether Class Members, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on affected individuals as a result of a data breach.

1958. PBI-Contracting Defendants therefore owed a duty to the PBI Bellwether Plaintiffs and PBI Bellwether Class Members to implement and maintain reasonable and adequate data security measures to secure, protect, and safeguard the PII entrusted to them by the PBI Bellwether Plaintiffs and PBI Bellwether Class Members.

1959. PBI-Contracting Defendants should have used their resources to implement and maintain adequate data security procedures and practices.

1960. PBI-Contracting Defendants breached their duties to the PBI Bellwether Plaintiffs and PBI Bellwether Class Members by, among other things, failing to employ adequate screening and vetting of their third-party vendors, including PBI.

1961. PBI-Contracting Defendants knew or should have known that PBI used Progress's MOVEit software to transfer and store their customers' and/or policyholders' PII.

1962. PBI-Contracting Defendants breached their duties to the PBI Bellwether Plaintiffs and PBI Bellwether Class Members by, among other things, failing to employ adequate screening and vetting of the software used by PBI to transfer and store their customers' and/or policyholders' PII.

1963. PBI-Contracting Defendants knew or should have known that Progress: (a) employed poorly written, outdated, and insecure code in its MOVEit software; (b) failed to update outdated code; and (c) failed to check for known or newly discovered vulnerabilities.

1964. PBI should have but did not vet Progress or its MOVEit Transfer software, and as a result, failed to prevent or detect the Data Breach. PBI-Contracting Defendants should have but did not vet PBI or the MOVEit Transfer software used by PBI to transfer and store their customers' and/or policyholders' PII. As a result, the PBI-Contracting Defendants failed to prevent or detect the Data Breach.

1965. PBI failed to ensure Progress employed and maintained adequate cybersecurity measures to prevent the Data Breach from occurring. PBI-Contracting Defendants failed to ensure PBI employed and maintained adequate cybersecurity measures to prevent the Data Breach from occurring.

1966. PBI had obligations arising under the FTC Act, industry standards, common law, and its own promises and representations made to the PBI-Contracting Defendants and to the PBI Bellwether Plaintiffs and PBI Bellwether Class Members to keep their PII confidential and protected from unauthorized access and disclosure. PBI-Contracting Defendants also had obligations arising under the FTC Act, Gramm-Leach-Bliley Act, industry standards, common law, and their own promises and representations made to the PBI Bellwether Plaintiffs and PBI Bellwether Class Members to keep their PII confidential and protected from unauthorized access and disclosure.

B. PBI Bellwether Defendants could have prevented the Data Breach.

1967. Several best practices have been identified that, at a minimum, PBI Bellwether Defendants should have implemented as companies that handle highly sensitive and confidential

PII in the regular course of their business operations. Yet, PBI Bellwether Defendants failed to do so. These best practices include, but are not limited to:

a. educating all employees about data security practices and procedures;

b. requiring strong passwords;

c. implementing multi-layer security—including firewalls, anti-virus, and anti-malware software;

d. adequately securing encryption keys;

e. multi-factor authentication;

f. backup data; and

g. limiting which employees can access sensitive data.

1968. Other standard cybersecurity practices that PBI Bellwether Defendants should have implemented, but failed to do so, include:

a. installing appropriate malware detection software;

b. monitoring and limiting the network ports;

c. protecting web browsers and email management systems;

d. setting up network systems such as firewalls, switches and routers;

e. monitoring and protection of physical security systems;

f. protection against any possible communication system; and

g. training staff regarding critical points.

1969. By virtue of the fact that the Data Breach occurred and resulted in millions of individuals' PII being compromised thereby, PBI Bellwether Defendants failed to meet the foregoing minimum standards, and/or of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security

Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness and should have been implemented and followed by the PBI Bellwether Defendants, yet they failed to do so.

1970. These foregoing frameworks are existing and applicable industry standards, and PBI Bellwether Defendants failed to comply with these accepted standards, thereby opening the door to Cl0p and causing the Data Breach.

1. Had PBI complied with applicable security standards, it would have determined that the MOVEit software was not safe to use and prevented the Data Breach

1971. PBI is responsible for protecting the PII it solicits and collects from attacks and breaches that result from weaknesses in third-party systems and software.

1972. PBI failed to safeguard the PBI Bellwether Plaintiffs' and Class Members' PII when it failed to adopt and enforce reasonable and available data security practices and procedures to prevent and/or mitigate the known risk of a cyberattack.

1973. Prior to the Data Breach, PBI should have, but did not, implement and maintain reasonable and necessary data security policies and procedures, which would have mitigated or avoided the Data Breach.

1974. There are numerous known and available steps that PBI could have taken to mitigate or even prevent the Data Breach.

1975. PBI could have prevented or mitigated against the risk of the Data Breach through implementation of security-standard data management, software review, data mapping, risk management, employment of zero-trust policies, and diligence concerning Progress's software.

1976. Data security practices that could and should have been implemented by PBI to prevent the MOVEit Data Breach include:

a. Auditing of third-party software, including the MOVEit Transfer software;

b. Vetting and periodic auditing of third-party vendors, including Progress;

c. Restricting MOVEit transfers to pre-approved IP addresses ("whitelisting");

d. Limiting the specific types of files that can be uploaded;

e. Conducting basic monitoring of web servers;

f. Using web application firewalls ("WAFs"); and

g. Employing supply chain security.

Each of the foregoing is explained in greater detail below.

2. Auditing Third-Party Software.

1977. Security audits of third-party software enable companies to identify vulnerabilities, monitor access to sensitive data, and discover and remediate any unauthorized data access.[587] Here, had PBI conducted security auditing of the MOVEit Transfer software, it could have prevented the Data Breach. The methods for conducting security audits of third-party software are well-known and widely available.[588] Security audits can detect security vulnerabilities, including SQL injection susceptibility. PBI therefore could and should have employed companies that conduct security audits of third-party software.[589]

3. Vetting Vendors.

1978. In addition to auditing third-party software, had PBI engaged in proper vetting and routine audits of vendors' data security practices, including vetting of Progress's cybersecurity practices, it could have prevented the Data Breach. Vendor risk assessments or security

[587] *6 Security Tips for Third Party* Software, Cybersecurity Insiders, https://www.cybersecurity-insiders.com/6-security-tips-for-third-party-software/ (last visited May 20, 2024).

[588] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard (updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software.

[589] Davit Asatryan, *Third-Party Applications Audit: Complete Guide*, Spin.ai (Nov. 4, 2021, updated Apr. 19, 2024), https://spinbackup.com/blog/third-party-applications-audit/.

questionnaires are "one of the best methods for extracting deep cybersecurity insights about any aspects of a vendor's attack surface."[590] Industry-standard risk assessments and security questionnaires designed to help companies discover vulnerabilities in third-party web applications and software are widely available,[591] and can be used to assess the security of third-party software against common attack vectors, including SQL injection susceptibility.[592]

4. Whitelisting.

1979. Had PBI restricted MOVEit transfers to pre-approved IP addresses—a cybersecurity practice referred to as "whitelisting"—it could also have prevented the Data Breach. A whitelist is an administrator-defined register of entities pre-approved for authorized access or to perform specific actions. Whitelisting enhances the security of a system or network by ensuring that only pre-approved users or devices have access to sensitive data or systems. Whitelisting thus denies access by default, providing authorization only to a vetted, pre-approved list of IP addresses, applications, email addresses, and/or users. PBI should have been able to implement a whitelist, as there were a limited number of users who needed to upload files to its MOVEit server. Blacklisting, in contrast, requires that known threats be specifically identified and blocked, while everything else is permitted. In a situation involving exploitation of a Zero-Day vulnerability, like

[590] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard (updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software ("Risk assessments can either be framework-based to identify security control deficiencies against popular security standards or custom-designed for focused investigations about specific third-party risks.").

[591] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard (updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software.

[592] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard (updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software.

the one Cl0p exploited in the MOVEit Data Breach, whitelisting is the preferred method. NIST Special Publication 800-167: *Guide to Application Whitelisting* provides specific guidance to companies on how to implement whitelisting.[593]

5. Limiting Specific File Types.

1980. Had PBI limited the specific types of files that could be uploaded via FTP, it could also have prevented the Data Breach. After exploiting the MOVEit vulnerability via SQL injection, Cl0p uploaded the LEMURLOOT web shell, which masqueraded as a legitimate file[594] and allowed the threat actor to execute commands, download files, extract system settings, and create/insert/delete users.[595]

1981. Proper data security dictates that only those files that are needed and expected to be uploaded should be allowed. This typically includes document file types such as .doc, .docx, .pdf, .xls, etc. Only web site administrators with whitelisted IP addresses should have been allowed to upload web page files, such as .aspx. Had PBI implemented that policy, the Data Breach could have been avoided.

---

[593] U.S. Dept. of Commerce, NIST Special Publication 800-167, *Guide to Application Whitelisting*, (Oct. 2015), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf.

[594] Kunal Modasiya, *Progress MOVEit Transfer Vulnerability Being Actively Exploited*, Qualys Blog (last updated Aug. 7, 2023), https://blog.qualys.com/vulnerabilities-threat-research/2023/06/07/progress-moveit-transfer-vulnerability-being-actively-exploited; *see also* Jonathan Reed, *The MOVEit breach impact and fallout: How can you respond?*, Security Intelligence (July 19, 2023), https://securityintelligence.com/news/the-moveit-breach-impact-and-fallout-how-can-you-respond/.

[595] U.S. Cybersecurity & Infrastructure Security Agency, Cybersecurity Advisory AA23-158A, *StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability* (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

6. Adequate Logging, Monitoring, and Auditing.

1982. "Logging, monitoring, and auditing procedures help an organization prevent incidents and provide an effective response when they occur."[596] These tools can detect SQL injection attempts and prevent breaches like the MOVEit Data Breach.

1983. Forensic examinations of the MOVEit Data Breach have confirmed that indicators of compromise were found in the logs of targeted organizations,[597] verifying that effective log monitoring would have mitigated or even prevented the Data Breach. Accordingly, PBI could and should have utilized commonly available tools that monitor logs automatically and provide alerts of unusual activity to administrators.

1984. "Several different logs record details of activity on systems and networks. For example, firewall logs record details of all traffic that the firewall blocked. By monitoring these logs, it's possible to detect incidents. Some automated methods of log monitoring automatically detect potential incidents and report them right after they've occurred."[598]

1985. Here, had PBI adequately logged and maintained log monitoring, it could have prevented the MOVEit Data Breach because such logs would have shown clear indicators of compromise and/or malicious activity. SQL injection attempts, successful or not, will appear in such logs. But even extensive logging is insufficient without adequate monitoring of said logs.

---

[596] Mike Chapple, et al., (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide (9th ed. 2021).

[597] Scott Downie, et al., *Transfer Vulnerability (CVE-2023-34362) Since 2021*, Kroll (June 8, 2023), https://www.kroll.com/en/insights/publications/cyber/clop-ransomware-moveit-transfer-vulnerability-cve-2023-34362.

[598] Darril Gibson, CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide at p. 73 (2017).

1986. The U.S. National Institute of Standards and Technology (NIST) publishes a Cybersecurity Framework that emphasizes continuous monitoring of systems.[599] The NIST SP 800-92 Guide to Computer Security Log Management further defines how to manage logs,[600] and there are a number of widely available tools that can monitor logs automatically and provide alerts to administrators when there is unusual activity.

1987. Had PBI monitored web server logs for new files—as recommended in NIST SP 800-12[601] as a widely accepted cybersecurity practice[602]—it would have promptly detected the new files introduced during the cyberattack and prevented the Data Breach. Web server monitoring would have specifically allowed PBI to detect the new files introduced to the web server root (human.aspx and human2.aspx) that enabled Cl0p to perpetrate the MOVEit Data Breach. Even basic monitoring of PBI's web servers could therefore have prevented the Data Breach because it would have revealed the backdoor Cl0p introduced to the web server.[603]

---

[599] U.S. Dept. of Commerce, *The NIST Cybersecurity Framework (CSF) 2*.0, Nat'l Inst. of Standards and Tech. (Feb. 26, 2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[600] U.S. Dept. of Commerce, NIST Special Publication 800-92, *Guide to Computer Security Log Management*, (Sept. 2006), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf.

[601] U.S. Dept. of Commerce, NIST Special Publication 800-12 rev.1, *An Introduction to Information Security*, (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

[602] *Monitor web server directories for changed / new files*, https://serverfault.com/questions/1145284/monitor-web-server-directories-for-changed-new-files (last visited May 20, 2024); *Gateway Script to monitor directory for new files*, Ignition, https://forum.inductiveautomation.com/t/gateway-script-to-monitor-directory-for-new-files/16124/5 (last visited May 20, 2024).

[603] Tyler Lioi, *MOVEit Transfer Investigations*, CrowdStrike Blog (June 5, 2023), https://www.crowdstrike.com/blog/identifying-data-exfiltration-in-moveit-transfer-investigations/.

1988. In addition to file system monitoring to identify new files, the InfoSec institute recommends: (a) network monitoring to identify rogue IP addresses which may be performing malicious activities such as brute-force or fuzzing; (b) authentication monitoring to identify unusual logins or login attempts; (c) file change monitoring to identify changes to sensitive files within the file system; and (d) process monitoring to identify rogue processes that might be malicious.[604] Had PBI implemented these steps, it could have prevented the Data Breach.

1989. Beyond monitoring activity, the actual data transferred via MOVEit could and should have been monitored by PBI. Most legitimate interactions utilizing MOVEit only upload or download relatively small amounts of data at a given time, but Cl0p was able to exfiltrate large amounts of consumer data in the Data Breach. Had PBI been adequately monitoring data transfers, any attempt to exfiltrate large amounts of data (significantly varying from normal usage) would have triggered an alert.

7. WAFs

1990. PBI could have implemented and maintained properly configured web application firewalls ("WAFs"), which could also have prevented the MOVEit Data Breach.[605]

8. Supply Chain Security

1991. Supply chain security is another common method of ensuring that all items in the supply chain, including third-party software like MOVEit, are secure.[606]

---

[604] Lester Obbayi, *Web server protection: Web server security monitoring*, InfoSec (May 4, 2020), https://www.infosecinstitute.com/resources/network-security-101/web-server-protection-web-server-security-monitoring/.

[605] *See, e.g.*, *Web Application Firewall*, Imperva, https://www.imperva.com/products/web-application-firewall-waf/ (last visited Apr. 26, 2024); *How Does WAF Detect SQL Injection, XSS, and PHP Injection Attacks?*, Huawei Cloud, (Sept. 6, 2023), https://support.huaweicloud.com/intl/en-us/waf_faq/waf_01_0457.html.

[606] U.S. Department of Commerce, NIST Conference Materials, *Best Practices in Cyber Supply Chain Risk Management*, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-

1992. The NIST explicitly discusses vulnerabilities in third party software[607] and provides three supply chain security principles[608] that, if applied, would have mitigated or prevented the MOVEit breaches:

Figure 15

Cyber Supply Chain Security Principles:

1. **Develop your defenses based on the principle that your systems will be breached**. When one starts from the premise that a breach is inevitable, it changes the decision matrix on next steps. The question becomes not just how to prevent a breach, but how to mitigate an attacker's ability to exploit the information they have accessed and how to recover from the breach.
2. **Cybersecurity is never just a technology problem, it's a people, processes and knowledge problem**. Breaches tend to be less about a technology failure and more about human error. IT security systems won't secure critical information and intellectual property unless employees throughout the supply chain use secure cybersecurity practices.
3. **Security is Security.** There should be no gap between physical and cybersecurity. Sometimes the bad guys exploit lapses in physical security in order to launch a cyber attack. By the same token, an attacker looking for ways into a physical location might exploit cyber vulnerabilities to get access.

9. Windows Security Feature

1993. Companies utilizing Windows have an additional protection modality. The Windows security system has ransomware protection, which allows the user to designate any folder as protected. Any attempt to add new files or change existing files in that folder would then have to be approved. Because LEMURLOOT masqueraded as a legitimate file that was then used

Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf (last visited May 20, 2024).

[607] U.S. Department of Commerce, NIST Conference Materials, *Best Practices in Cyber Supply Chain Risk Management*, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf (last visited May 20, 2024).

[608] U.S. Department of Commerce, NIST Conference Materials, *Best Practices in Cyber Supply Chain Risk Management*, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf (last visited May 20, 2024).

as a backdoor, having the folder \inetpub\wwwroot\ protected from alterations would have prevented these files from being uploaded.

1994. In addition to the foregoing data security practices, which, if adopted by PBI, could have prevented the Data Breach, there are a number of common security techniques and mechanisms that should be a part of any standard data security policy and could have limited the scope of damage from a data breach. These security techniques and practices include:

a. Limiting access by employing a "least privileges" policy;

b. Implementing "Zero Trust" security frameworks;

c. Encrypting data at rest and adequately securing the encryption keys so that the data cannot be decrypted by unauthorized users; and

d. Immediately applying patches once they were made available.

1995. A "least privileges" policy can limit an attacker who exploits a vulnerability from accessing large volumes of data. Limiting access via policies such as least privileges means that, even if a threat actor is able to exploit a vulnerability or even use a legitimate login to access the system, access to sensitive data will be limited. The large volume of records accessed and exfiltrated from PBI's MOVEit Transfer server in the Data Breach indicates that this was not done, because it is highly unlikely that any login would have legitimate access to that amount of sensitive data.

1996. "Zero Trust" is a security model and set of system design principles that emphasize security verification in network environments. The core principle of Zero Trust is "never trust, always verify." Thus, unlike traditional security models that assume everything inside a network is safe, Zero Trust assumes threats can exist both inside and outside the network.

1997. Zero Trust security frameworks require all users, whether inside or outside the organization's network, to be authenticated, authorized, and continuously validated for security

configuration and posture before being granted access to applications and data.[609] Numerous standards provide guidelines to organizations implementing Zero Trust security frameworks, including NIST SP 800-207,[610] NIST SP 800-205,[611] and the CISA zero trust maturity model.[612]

1998. Two aspects of Zero Trust are particularly applicable to the MOVEit Data Breach. The first is the network is segmented into smaller, secure zones to maintain separate access for different parts of the network. This reduces the lateral movement of attackers within the network. The second is continuously monitoring the security posture of all hardware and software on the network. This helps to detect and respond to threats in real time.

1999. The United States Cybersecurity & Infrastructure Security Agency published recommendations for mitigating the MOVEit vulnerability by "[g]rant[ing] admin privileges and access only when necessary, [and] establishing a software allow list that only executes legitimate applications."[613]

---

[609] *See, e.g.*, *Zero Trust, A revolutionary approach to Cyber or just another buzz word?*, Deloitte (2021), https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/deloitte-cyber-zero-trust.pdf; *see also* Venu Shastri, *Zero Trust Architecture*, CrowdStrike (June 28, 2023), https://www.oracle.com/security/what-is-zero-trust; https://www.crowdstrike.com/cybersecurity-101/zero-trust-security.

[610] U.S. Department of Commerce, NIST Special Publication 800-207, *Zero Trust Architecture*, CSRC (Aug. 2020), https://csrc.nist.gov/pubs/sp/800/207/final.

[611] U.S. Department of Commerce, NIST Special Publication 800-205, *Attribute Considerations for Access Control Systems*, CSRC (June 2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-205.pdf.

[612] U.S. Cybersecurity & Infrastructure Security Agency, *Zero Trust Maturity Model* (Apr. 2023), https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf.

[613] U.S. Cybersecurity & Infrastructure Security Agency, Cybersecurity Advisory AA23-158A, *StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability* (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

2000. Following Progress's announcement of the first MOVEit vulnerability on May 31, 2023,[614] PBI should have, but did not, immediately begin taking security measures. PBI's failure to adequately safeguard the PBI Bellwether Plaintiffs' and Class Members' PII resulted in that information being accessed or obtained by third-party cybercriminals.

C. PBI failed to follow Progress's recommendations regarding secure configuration of the MOVEit software, which further contributed to the Data Breach.

2001. The MOVEit software offers secure configurations that any customer could implement to make the system more secure and to mitigate the ultimate impact of this Breach.

2002. Progress made several additional recommendations to users of the MOVEit software (listed below), yet—by virtue of the occurrence of the Data Breach—PBI clearly failed to implement:

a. Using consistency check and tamper check utilities to validate consistency and the audit log.

b. Review audit logs for any anomalous behavior. Such anomalous behavior includes:

   i. Sign-ons from specific IP addresses

   ii. APIs used

   iii. Modification of settings

c. Limiting administrative privileges[615]

---

[614] *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)*, Progress (last updated June 15, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023.

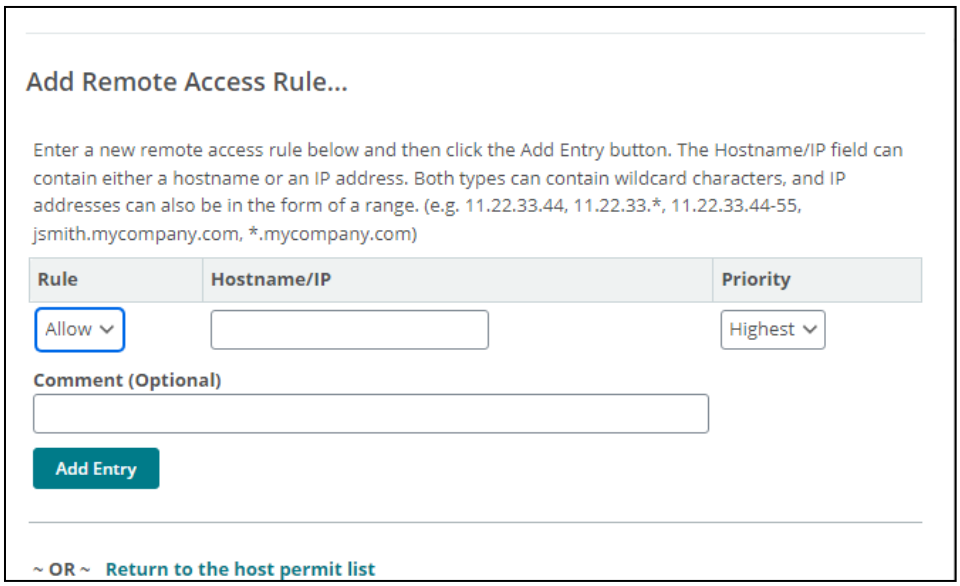
[615] *Progress Documentation: MOVEit Transfer 2022 Administrator Guide*, Progress (updated Apr. 6, 2022), https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/Permissions_3.html.

d. IP and user lockout policies[616]

e. Whitelisting so only specific IP addresses and users could login remotely.[617]

2003. PBI could and should have turned on whitelisting, as depicted below:

Figure 16

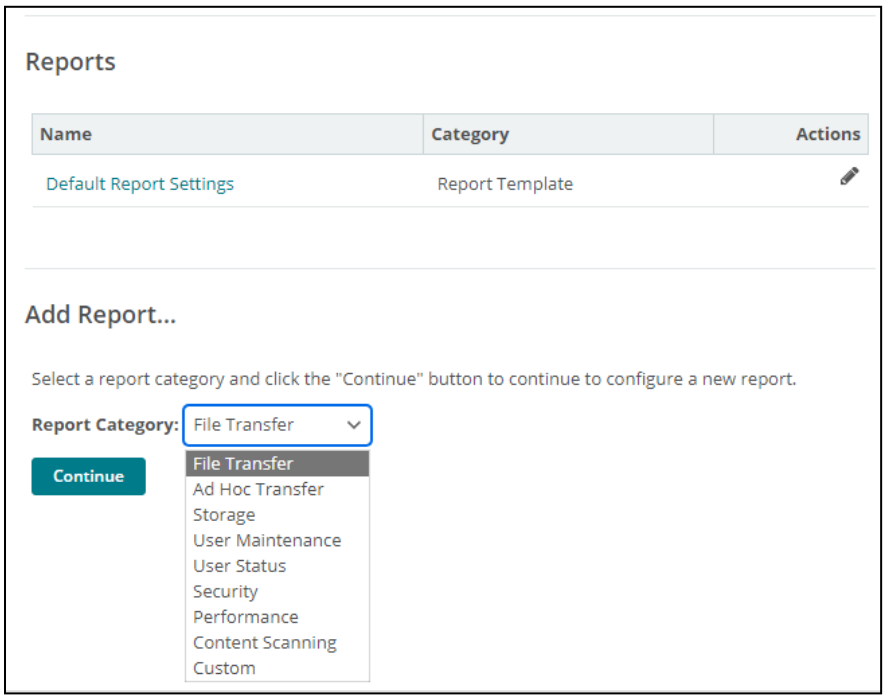


2004. Generating reports in MOVEit is also a simple process, as depicted below:

[616] *Progress Documentation: MOVEit Automation Web Admin Help – IP/User Lockout Policy*, Progress (updated Feb. 21, 2022), https://docs.progress.com/bundle/moveit-automation-web-admin-help-2022/page/IPUser-Lockout-Policy.html.

[617] *MOVEit Transfer – Whitelist IP for Specific Users Accounts*, Progress: Community (Oct. 14, 2020), https://community.progress.com/s/article/moveit-transfer-whitelist-ip-for-specific-users-accounts.

Figure 17



2005. There are a number of security reports built into the MOVEit software:

Figure 18

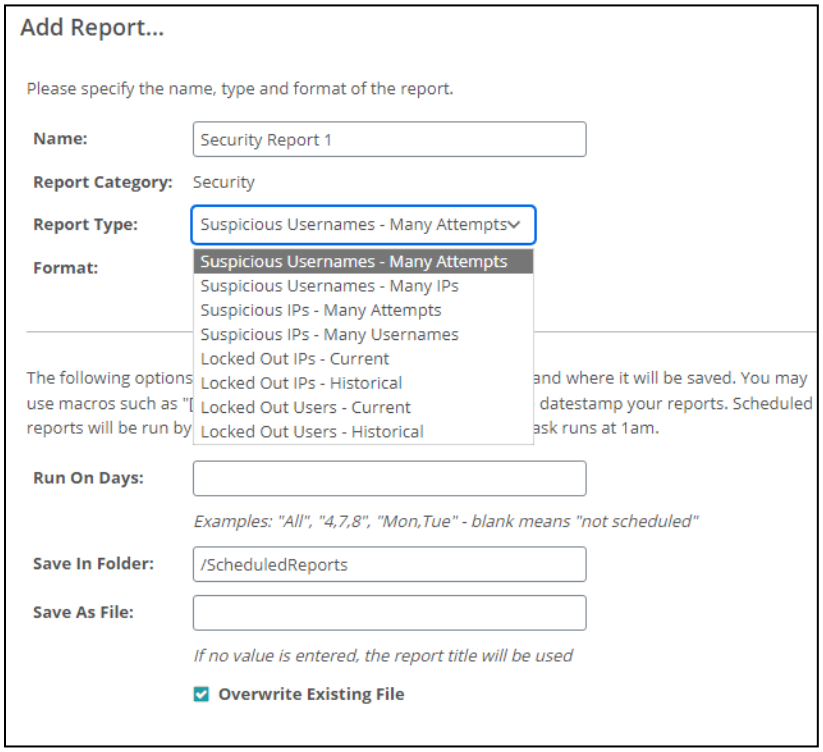
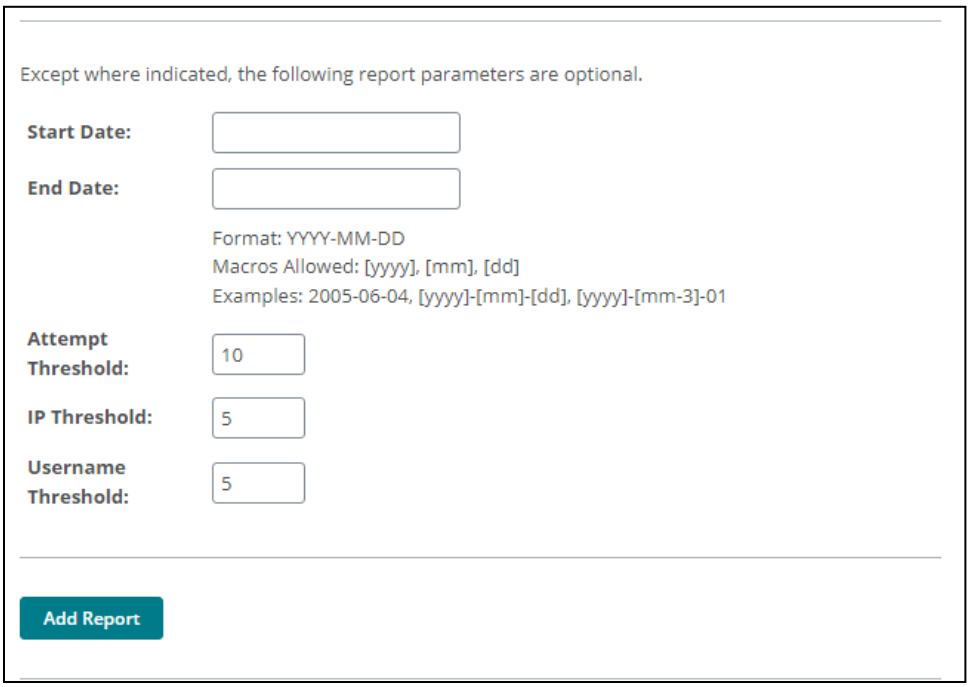
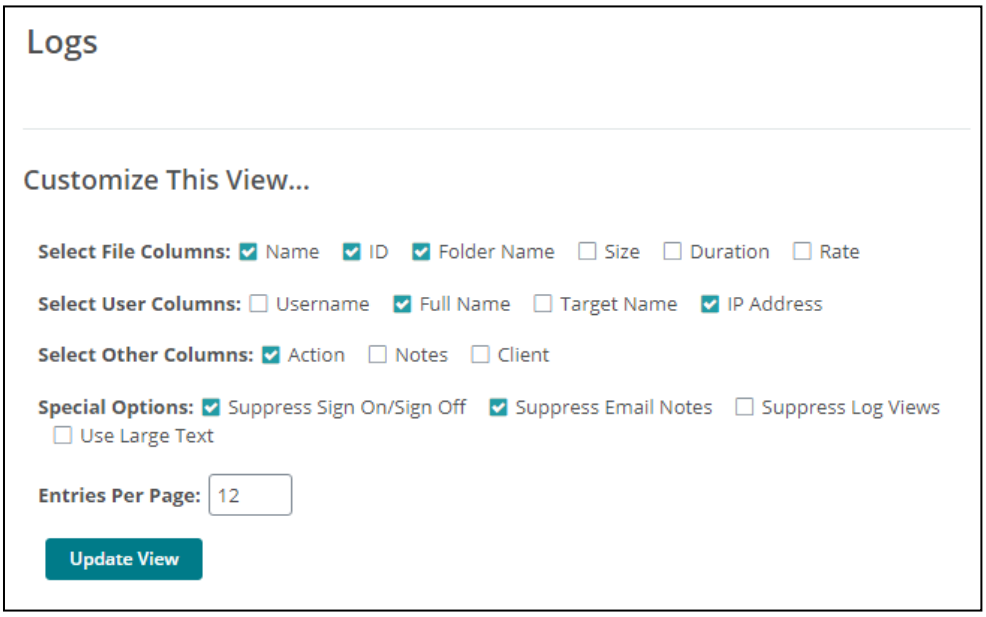


Figure 19



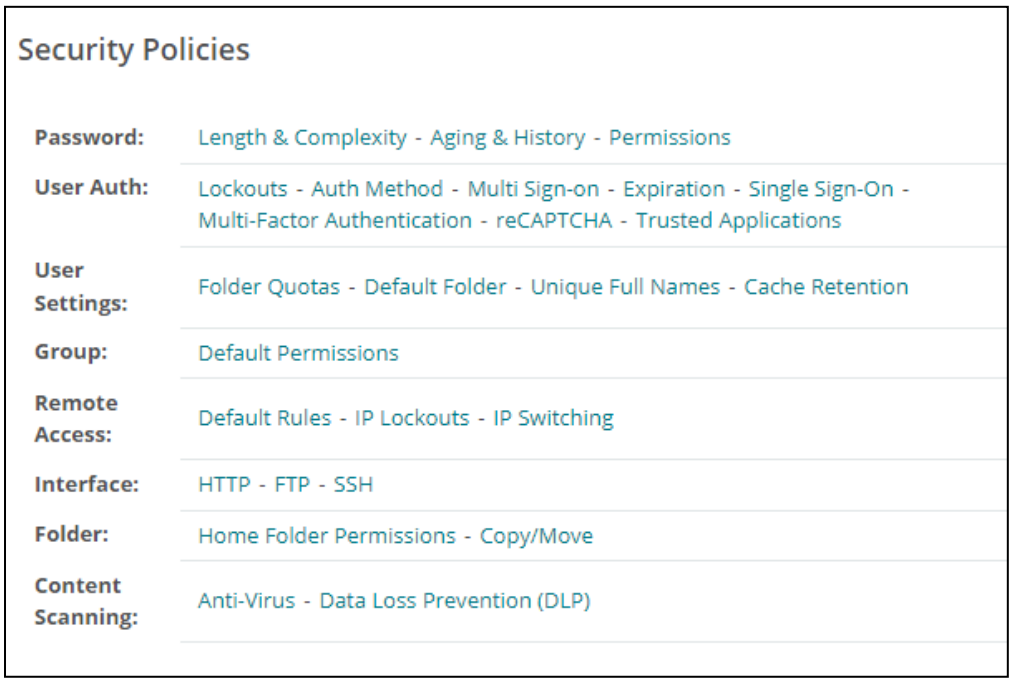
2006. MOVEit users can also customize the view of logs:

Figure 20



2007. A number of additional security policies can be set with a simple point and click:

Figure 21



2008. Data loss prevention rules could and should have been enabled to prevent exfiltration of data:

Figure 22

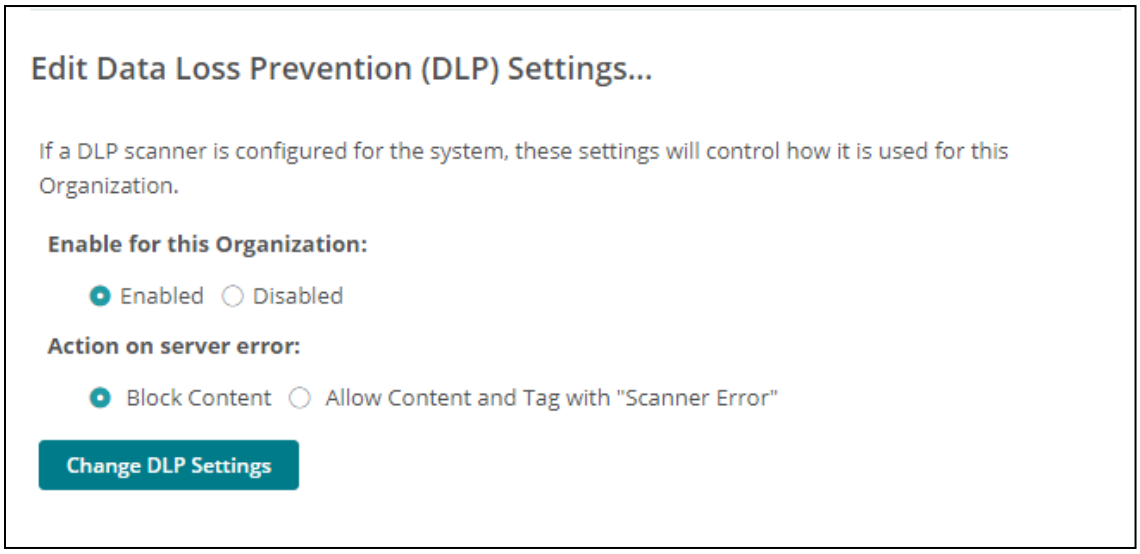


Figure 23

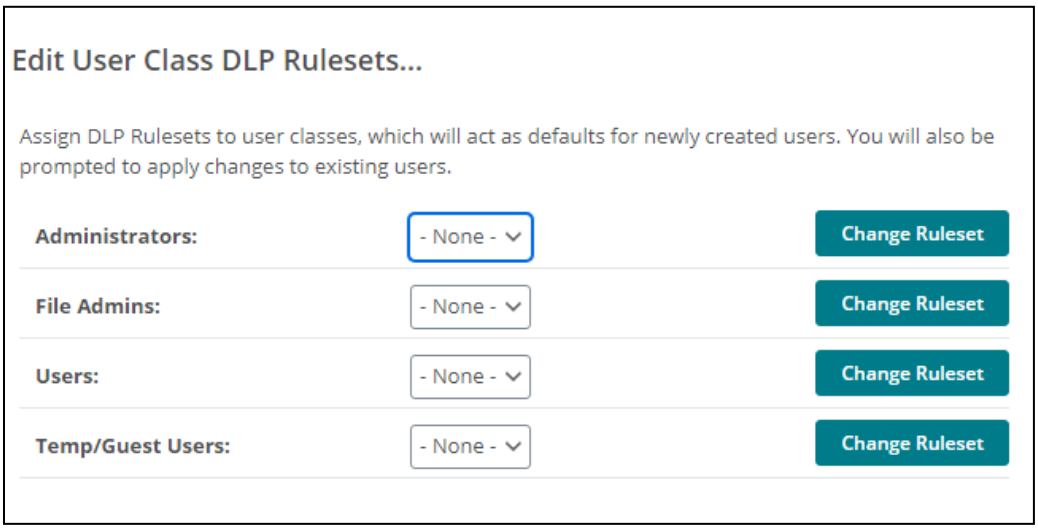
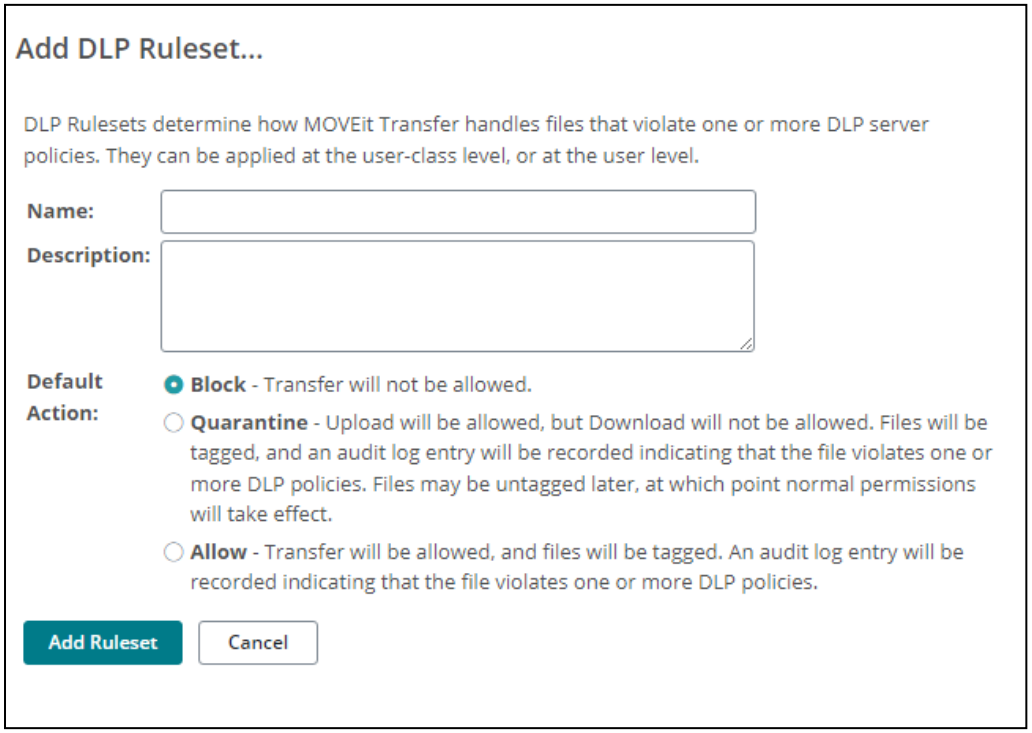


Figure 24



2009. It is unclear which, if any, of these security measures were implemented by PBI.

D. Had PBI-Contracting Defendants complied with applicable security standards, they would have determined that the MOVEit software was not safe to use and prevented the Data Breach.

2010. The PBI-Contracting Defendants are responsible for protecting the PII they solicit and collect from attacks and breaches that result from weaknesses in third-party systems and software.

2011. The PBI-Contracting Defendants failed to safeguard the PBI Bellwether Plaintiffs' and Class Members' PII when they failed to adopt and enforce reasonable and available data security practices and procedures to prevent and/or mitigate the known risk of a cyberattack.

2012. Prior to the Data Breach, the PBI-Contracting Defendants should have, but did not, implement and maintain reasonable and necessary data security policies and procedures, which would have mitigated or avoided the Data Breach.

2013. There are numerous known and available steps that the PBI-Contracting Defendants could have taken to mitigate or even prevent the Data Breach.

2014. Data security practices that could and should have been implemented by the PBI-Contracting Defendants to prevent the MOVEit Data Breach include:

a. Vetting and periodic auditing of third-party vendors, including PBI and Progress;

b. Auditing of third-party software, including the MOVEit Transfer software; and

c. Employing supply chain security.

Each of these three measures—and the PBI-Contracting Defendants' failure to utilize them—are explained in greater detail below:

1. Auditing Third-Party Vendors and Software

2015. Security audits of third-party vendors and third-party software enable companies to identify vulnerabilities, monitor access to sensitive data, and discover and remediate any unauthorized data access.[618]

2016. The PBI-Contracting Defendants should have but did not properly vet or audit their third-party vendors, including PBI.

2017. The PBI-Contracting Defendants knew or should have known that PBI used the MOVEit Transfer software to transfer and/or store their customers' and policyholders' PII.

2018. Security auditing of PBI and the MOVEit Transfer software could have prevented the Data Breach as to the PBI-Contracting Defendants.

2019. The methods for conducting security audits of third-party vendors and software are well-known and widely available.[619]

2020. The PBI-Contracting Defendants therefore could and should have employed companies that conduct security audits of third-party vendors and third-party software.[620]

2. Vetting Vendors

2021. PBI-Contracting Defendants could have prevented the Data Breach by engaging in the standard industry practice of vetting vendors—such as PBI—that they transferred highly

[618] *6 Security Tips for Third Party Software*, Cybersecurity Insiders, https://www.cybersecurity-insiders.com/6-security-tips-for-third-party-software/ (last visited May 20, 2024).

[619] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard (updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software.

[620] Davit Asatryan, *Third-Party Applications Audit: Complete Guide*, Spin.ai (Nov. 4, 2021, updated Apr. 19, 2024), https://spinbackup.com/blog/third-party-applications-audit/.

sensitive PII to. Had PBI-Contracting Defendants done so, they would have discovered the vulnerability used by C10p and prevented the Data Breach. They failed to do so.

2022. Vendor risk assessments or security questionnaires are "one of the best methods for extracting deep cybersecurity insights about any aspects of a vendor's attack surface."[621] Industry-standard risk assessments and security questionnaires designed to help companies discover vulnerabilities in third-party web applications and software are widely available,[622] and can be used to assess the security of third-party software against common attack vectors, including SQL injection susceptibility.[623] Proper vetting and routine audits of vendors' data security practices, including vetting of PBI's and Progress's cybersecurity practices, could have prevented the Data Breach. PBI and the PBI-Contracting Defendants chose to use the MOVEit software to transfer sensitive information despite its security flaws, and failed to take the simple, industry-standard step of vetting the MOVEit service before using it to transfer millions of pieces of highly sensitive PII.

2023. Further, by failing to take the various steps alleged above (including thoroughly vetting the MOVEit software), PBI and the PBI-Contracting Defendants enriched themselves by

[621] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard (updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software ("Risk assessments can either be framework-based to identify security control deficiencies against popular security standards or custom-designed for focused investigations about specific third-party risks.").

[622] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard (updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software.

[623] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard (updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software.

saving the costs they reasonably should have expended on adequate data security measures to secure the PBI Bellwether Plaintiffs' and Class Members' PII.

2024. Instead of providing a reasonable level of security that would have prevented the Data Breach, PBI and the PBI-Contracting Defendants instead calculated to avoid their data security obligations at the expense of the PBI Bellwether Plaintiffs and PBI Bellwether Class Members by utilizing cheaper, ineffective security measures. The PBI Bellwether Plaintiffs and PBI Bellwether Class Members, on the other hand, suffered as a direct and proximate result of the PBI Bellwether Defendants' failures to provide the requisite security.

E. PBI's failure to comply with laws and industry standards mandating that it act as quickly as possible in response to the Data Breach led to additional losses.

2025. PBI's failures were compounded by its inadequate response to the Data Breach.

2026. According to PBI, Cl0p accessed and downloaded data from one of its MOVEit Transfer servers—which housed highly-sensitive consumer information entrusted to PBI by the PBI-Contracting Defendants—on May 29, 2023, and May 30, 2023.[624]

2027. PBI "became aware of the MOVEit [Data Breach] on June 2, 2023,"[625] but failed to promptly notify the PBI-Contracting Defendants of the Breach.

2028. PBI claims to understand "the importance of notifying individuals who may have had their sensitive personally identifiable information acquired by an unauthorized [third

[624] *Data Breach Notifications – Pension Benefit Information, LLC*, Office of the Maine Attorney General (July 11, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/14efac97-4a7c-4322-98eb-2e953884eb58/f135d329-507c-484c-9798-b46d470c5d96/Notice%20of%20Data%20Event%20-%20PBI%20-%20ME.pdf.

[625] PBI, *Global MOVEit Transfer Cyberattack*, https://www.pbinfo.com/faq-communication/ (last accessed Oct. 21, 2024).

party],"[626] but waited at least two weeks after first learning of the Data Breach to begin notifying the PBI-Contracting Defendants that their customers' PII may have been stolen in the Data Breach.[627] After PBI notified the PBI-Contracting Defendants of the Data Breach, it took PBI and each of the PBI-Contracting Defendants several additional weeks to begin notifying impacted individuals that their Private Information had been stolen by Cl0p.

2029. PBI waited until June 16, 2023 to notify Genworth about the Data Breach,[628] and waited another two months to begin notifying the 2.5 to 2.7 million Genworth customers and insurance agents whose PII was stolen by Cl0p in the Data Breach.[629] According to Genworth, "PBI [] mail[ed] notification letters [to impacted Genworth customers and insurance agents] in batches through the month of August [2023][.]"[630]

2030. PBI also waited until June 16, 2023, to notify Milliman about the Data Breach,[631] and waited another month to begin notifying the 1.3 million Milliman customers whose PII was

---

[626] PBI, *Privacy Principles*, https://www.pbinfo.com/privacy-principles/ (last accessed Oct. 18, 2024).

[627] *See, e.g.*, *MOVEit Security Event*, Genworth (last updated Aug. 31, 2023), https://www.genworth.com/moveit#backgroundinfo; *Data Breach Notifications – Milliman Solutions LLC*, Office of the Maine Attorney General (July 17, 2023), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a98d9ae9-b898-4aaa-8dde-de04551aaedb.shtml.

[628] *See MOVEit Security Event*, Genworth (last updated Aug. 31, 2023), https://www.genworth.com/moveit#backgroundinfo.

[629] *MOVEit Security Event – Background Information*, Genworth (last updated Aug. 31, 2023), https://www.genworth.com/moveit#backgroundinfo.

[630] *MOVEit Security Event – Background Information*, Genworth (last updated Aug. 31, 2023), https://www.genworth.com/moveit#backgroundinfo.

[631] *Data Breach Notifications – Milliman Solutions LLC*, Office of the Maine Attorney General (July 17, 2023), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a98d9ae9-b898-4aaa-8dde-de04551aaedb.shtml; *see also* Milliman, *Data Breach Notice* (July 17, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/a98d9ae9-b898-4aaa-8dde-de04551aaedb/af45f431-a61c-4c76-9d70-f31ab3236aa7/PBI%20-%20Sample%20Notification%20Letter.pdf.

stolen from PBI's MOVEit Transfer server.[632] According to Milliman, Milliman clients' customers were not notified of the Data Breach until July 17, 2023—nearly seven weeks after their highly-sensitive data had fallen into the hands of cybercriminals.[633] Some Milliman customers were notified even later, after PBI completed an additional "review on July 21, 2023, and confirmed to Milliman at that time that the personal information of certain [additional] consumers of Milliman's clients were affected[.]"[634] PBI did not begin notifying those individuals until August 14, 2023—more than two and a half months after their highly-sensitive information was stolen in the Data Breach.[635]

2031. PBI waited until June 19, 2023, to confirm that "TIAA files had been exfiltrated"[636] from one of its MOVEit Transfer servers in the Data Breach. In turn, TIAA did not confirm which

---

[632] *Data Breach Notifications – Milliman Solutions LLC*, Office of the Maine Attorney General, (June 16, 2023), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a98d9ae9-b898-4aaa-8dde-de04551aaedb.shtml.

[633] *See Data Breach Notifications – Milliman Solutions LLC*, Office of the Maine Attorney General, (June 16, 2023), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/a98d9ae9-b898-4aaa-8dde-de04551aaedb.shtml (noting "Date(s) of consumer notification: **Starting 07/17/2023**) (emphasis in original); *see also PBI Sample Notification Letter*, Milliman (July 17, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/a98d9ae9-b898-4aaa-8dde-de04551aaedb/af45f431-a61c-4c76-9d70-f31ab3236aa7/PBI%20-%20Sample%20Notification%20Letter.pdf.

[634] *Letter to the Office of the Maine Attorney General*, Milliman (August 14, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/903ecb46-93b2-4986-aae5-ec7e088625f8/31ce7f5a-a49a-48eb-a52b-33dd1d68bc1a/23.08.14%20ME%20AG%20Notification%20Letter.pdf.

[635] *Data Breach Notifications – Milliman Solutions LLC*, Office of the Maine Attorney General (August 14, 2023), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/903ecb46-93b2-4986-aae5-ec7e088625f8.shtml.

[636] *Notice of Data Security Incident*, TIAA (July 21, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/ed67df63-aced-4ecb-91ce-602c7e34c83a/573351f0-74fc-4e19-9a62-a51fb837a3bb/Regulator%20Notice%20-%20TIAA%20ME%20AG.pdf.

of its customers were impacted by the Breach until June 28, 2023.[637] According to TIAA, PBI did not begin sending data breach notice letters to the 2.6 million TIAA participants whose PII was stolen by Cl0p until July 14, 2023, and the letters were sent "on a rolling basis over the [following] three weeks[.]"[638]

2032. PBI's delayed disclosure of the MOVEit Data Breach prevented its business clients, including the PBI-Contracting Defendants, from taking prompt action, including discontinuing use of PBI's MOVEit administrative portal as a "secure" file transfer application.

2033. Following the Data Breach, PBI reassured its business clients, including the PBI-Contracting Defendants, that they could "continue to safely do business with PBI" because "PBI systems were not impacted[.]"[639]

2034. But the zero-day vulnerability that was exploited by Cl0p in the Data Breach was not the only critical vulnerability in the MOVEit Transfer software. In the months following Progress's May 31, 2023 announcement of CVE-2023-34362,[640] Progress disclosed six additional

---

[637] *Notice of Data Security Incident*, TIAA (July 21, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/ed67df63-aced-4ecb-91ce-602c7e34c83a/573351f0-74fc-4e19-9a62-a51fb837a3bb/Regulator%20Notice%20-%20TIAA%20ME%20AG.pdf.

[638] *Notice of Data Security Incident*, TIAA (July 21, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/ed67df63-aced-4ecb-91ce-602c7e34c83a/573351f0-74fc-4e19-9a62-a51fb837a3bb/Regulator%20Notice%20-%20TIAA%20ME%20AG.pdf.

[639] PBI, *Global MOVEit Transfer Cyberattack*, https://www.pbinfo.com/faq-communication/ (last accessed Oct. 21, 2024).

[640] U.S. Department of Commerce, NIST, *Progress MOVEit Transfer SQL Injection Vulnerability (CVE-2023-34362) Detail*, Nat'l Vulnerability Database (updated Apr. 25, 2024), https://nvd.nist.gov/vuln/detail/CVE-2023-34362.

SQL injection vulnerabilities, each of which would allow a malicious threat actor to access and exfiltrate sensitive data from MOVEit Transfer servers.[641]

2035. Still, PBI failed to advise its business clients, including the PBI-Contracting Defendants, to discontinue use of its MOVEit administrative portal as a "secure" file transfer application.

2036. Instead, PBI "encourage[d]"—but did not require—"[its] customers to encrypt files prior to uploading"[642] them to PBI's MOVEit Transfer server.

2037. On August 14, 2023, more than two and a half months after the Data Breach, Milliman reported that Milliman "ha[d] stopped transferring data to PBI pending further evaluation of PBI's information security practices."[643]

---

[641] See, e.g., Threat Brief – MOVEit Transfer SQL Injection Vulnerabilities: CVE-2023-34362, CVE-2023-35036 and CVE-2023-34362, CVE-2023-35036 and CVE-2023-35708, Unit 42 (updated Oct. 4, 2023), https://unit42.paloaltonetworks.com/threat-brief-moveit-cve-2023-34362/; NIST, Progress MOVEit Transfer SQL Injection Vulnerability (CVE-2023-35036) Detail, Nat'l Vulnerability Database (updated Apr. 25, 2024), https://nvd.nist.gov/vuln/detail/CVE-2023-35036; NIST, Progress MOVEit Transfer SQL Injection Vulnerability (CVE-2023-35708) Detail, Nat'l Vulnerability Database (updated Apr. 25, 2024), https://nvd.nist.gov/vuln/detail/CVE-2023-35708; NIST, Progress MOVEit Transfer SQL Injection Vulnerability (CVE-2023-36934) Detail, Nat'l Vulnerability Database (updated Apr. 25, 2024), https://nvd.nist.gov/vuln/detail/CVE-2023-36934 (CVE-2023-36934 is a critical, unauthenticated SQL injection vulnerability); NIST, Progress MOVEit Transfer SQL Injection Vulnerability (CVE-2023-36932) Detail, Nat'l Vulnerability Database (updated Apr. 25, 2024), https://nvd.nist.gov/vuln/detail/CVE-2023-36932 (CVE-2023-36932 is a high-severity SQL injection vulnerability that could allow authenticated attackers to gain access to the MOVEit Transfer database).

[642] PBI, *Global MOVEit Transfer Cyberattack*, https://www.pbinfo.com/faq-communication/ (last accessed Oct. 21, 2024).

[643] *Letter to the Office of the Maine Attorney General*, Milliman (August 14, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/903ecb46-93b2-4986-aae5-ec7e088625f8/31ce7f5a-a49a-48eb-a52b-33dd1d68bc1a/23.08.14%20ME%20AG%20Notification%20Letter.pdf.

2038. Genworth and TIAA continued to transfer their customers' highly sensitive PII to PBI, and that information continued to be stored on PBI's MOVEit Transfer server, even after PBI learned of the critical vulnerabilities in the MOVEit Transfer code.

2039. PBI's delayed disclosure of the MOVEit Data Breach to the PBI-Contracting Defendants, and the further delayed notifications to the PBI-Contracting Defendants' customers, prevented the PBI Bellwether Plaintiffs and Class Members from taking prompt action to protect themselves from the fallout of the Data Breach.

2040. PBI and the PBI-Contracting Defendants failed to comply with legal and regulatory requirements to promptly notify impacted individuals following a data breach, including the laws of several states, which mandate that timely notices be sent to consumers following a data breach "in the most expedient time and manner possible and without unreasonable delay[.]"[644]

2041. The PBI Bellwether Plaintiffs and Class Members were not notified of the Data Breach until at least seven weeks—and in some cases, several months—after their PII had been stolen by Cl0p.

2042. The PBI Bellwether Defendants' failures to disclose the Data Breach in a timely and accurate manner was misleading and deceptive, because the PBI Bellwether Plaintiffs and Class Members reasonably believed their PII was adequately secured by the PBI-Contracting Defendants and PBI, due to the sensitive nature of the data, the nature of their relationship with the PBI-Contracting Defendants, and the explicit promises made by PBI and the PBI-Contracting Defendants concerning their data security practices and safeguards.

[644] California Civil Code § 1798.82(a); *see also Data Breach Notification Laws by State*, IT Governance USA, https://www.itgovernanceusa.com/data-breach-notification-laws (last accessed Nov. 1, 2024).

2043. As victims of the MOVEit Data Breach, the PBI Bellwether Plaintiffs and Class Members faced immediate and significant harms.

2044. The delayed notice letters that PBI sent to the PBI Bellwether Plaintiffs and Class Members, on behalf of the PBI-Contracting Defendants, indicate that PBI and the PBI-Contracting Defendants recognize the present and continuing risk of identity theft and fraud that the PBI Bellwether Plaintiffs and Class Members face as a result of the Data Breach.

2045. In the notice letters sent to individual consumers on behalf of PBI's business clients, including the PBI-Contracting Defendants, PBI "encourage[d] [impacted individuals] to remain vigilant against incidents of identity theft and fraud by reviewing [their] account statements and monitoring [their] free credit reports for suspicious activity and to detect errors."[645]

2046. Had the PBI Bellwether Defendants not delayed in notifying the PBI Bellwether Plaintiffs and Class Members about the Data Breach, Plaintiffs and Class Members could have immediately taken these and other precautions to protect their identities and mitigate the harms of the Data Breach.

2047. Instead, the PBI Bellwether Plaintiffs and Class Members were entirely unaware that their PII had fallen into the hands of cybercriminals for several weeks or months after the Data Breach.

2048. The PBI Bellwether Plaintiffs and Class Members have already suffered harms caused by the fraudulent or attempted misuse of their PII, and remain at an imminent and ongoing risk of additional future harm from identity theft and fraud.

---

[645] *Data Breach Notifications – Pension Benefit Information, LLC,* Office of the Maine Attorney General (July 11, 2023), https://www.maine.gov/ag/attachments/985235c7-cb95-4be2-8792-a1252b4f8318/14efac97-4a7c-4322-98eb-2e953884eb58/f135d329-507c-484c-9798-b46d470c5d96/Notice%20of%20Data%20Event%20-%20PBI%20-%20ME.pdf.

2049. The PBI Bellwether Defendants' unreasonable delays in notifying affected individuals following the Data Breach compounded the harms suffered by the PBI Bellwether Plaintiffs and Class Members.

F. PBI Bellwether Defendants Failed to Comply with FTC Guidelines.

2050. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Additionally, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236 (3d Cir. 2015).

2051. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

2052. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for

suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

2053. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

2054. These FTC enforcement actions include actions against financial institutions, like PBI Bellwether Defendants Genworth, Milliman, and MLIC.

2055. As evidenced by the Data Breach, PBI Bellwether Defendants failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of their vendors' data security practices. PBI Bellwether Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

2056. PBI Bellwether Defendants were at all times fully aware of their obligation to protect the PII of their customers yet failed to comply with such obligations. PBI Bellwether Defendants were also aware of the significant repercussions that would result from their failure to do so.

G. PBI Bellwether Defendants Genworth, Milliman, MLIC, and TIAA Failed to Comply with the Gramm-Leach Bliley Act.

2057. PBI Bellwether Defendants Genworth, Milliman, MLIC, and TIAA are financial institutions, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus are subject to the GLBA.

2058. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

2059. Genworth, Milliman, MLIC, and TIAA collect nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period, Genworth, Milliman, MLIC, and TIAA were subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq*., and are subject to numerous rules and regulations promulgated on the GLBA statutes.

2060. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

2061. Accordingly, Genworth, Milliman, MLIC, and TIAA's conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

2062. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must

include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, PBI Bellwether Defendants Genworth, Milliman, MLIC, and TIAA violated the Privacy Rule and Regulation P.

2063. Genworth, Milliman, MLIC, and TIAA failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing that PII on their network systems as well as those of their vendors.

2064. Genworth, Milliman, MLIC, and TIAA failed to adequately inform their customers that they were storing and/or sharing, or would store and/or share, the customers' PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the customer relationship ended.

2065. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified by risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key

controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

2066. As alleged herein, PBI Bellwether Defendants Genworth, Milliman, MLIC, and TIAA violated the Safeguards Rule.

2067. Genworth, Milliman, MLIC, and TIAA failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information and failed to monitor the systems of their vendors or verify the integrity of those systems.

2068. PBI Bellwether Defendants Genworth, Milliman, MLIC, and TIAA violated the GLBA and their own policies and procedures by sharing the PII of PBI Bellwether Plaintiffs and PBI Bellwether Class Members with a non-affiliated third party without providing PBI Bellwether Plaintiffs and PBI Bellwether Class Members: (a) an opt-out notice, and (b) a reasonable opportunity to opt out of such disclosure.

H. Damages Sustained by PBI Bellwether Plaintiffs and the PBI Bellwether Class Members.

2069. PBI Bellwether Plaintiffs and all other PBI Bellwether Class Members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft and medical theft—a risk that justifies expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

2070. For all of the foregoing reasons set forth in detail above in Chapter Three, PBI is directly liable to every member of the PBI Class and faces substantial exposure—both individually and via joint and several liability—as the primary defendant in the claims stemming from PBI's use of MOVEit and the Data Breach that impacted PBI. PBI is able to satisfy actual or potential judgments on behalf of the PBI Class. PBI further faces actual and potential indemnification/ contribution claims from all users of its services, including but not limited to all PBI-VCE and PBI-VCEC defendants (including but not limited to those listed in Ex. A, ECF No. 1161-1, at 4-6 (beneath the header "Vendor: Pension Benefit Information").

III. PBI BELLWETHER CLASS ALLEGATIONS

2071. PBI Bellwether Plaintiffs bring this action on behalf of themselves and, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) as representatives of the following classes:

> PBI Nationwide Class: All persons whose PII was compromised on PBI's platform and/or systems in the MOVEit Data Breach.
>
> > PBI California Class: All residents of California whose PII was compromised on PBI's platform and/or systems in the MOVEit Data Breach.
> >
> > PBI Florida Class: All residents of Florida whose PII was compromised on PBI's platform and/or systems in the MOVEit Data Breach.
> >
> > PBI Illinois Class: All residents of Illinois whose PII was compromised on PBI's platform and/or systems in the MOVEit Data Breach.
> >
> > PBI New Jersey Class: All residents of New Jersey whose PII was compromised on PBI's platform and/or systems in the MOVEit Data Breach.
> >
> > PBI New York Class: All residents of New York whose PII was compromised on PBI's platform and/or systems in the MOVEit Data Breach.

PBI Pennsylvania Class: All residents of Pennsylvania whose PII was compromised on PBI's platform and/or systems in the MOVEit Data Breach.

PBI Texas Class: All residents of Texas whose PII was compromised on PBI's platform and/or systems in the MOVEit Data Breach.

PBI Vermont Class: All residents of Vermont whose PII was compromised on PBI's platform and/or systems in the MOVEit Data Breach.

The foregoing state-specific PBI classes are collectively referred to as the "PBI State Classes."

2072. Additionally, PBI Bellwether Plaintiffs Bailey, Camille Burgan, Eugene Burgan, Gilbert Hale, Lynda Hale, Hauser, and Hernandez (collectively, "Genworth Plaintiffs") bring this action on behalf of themselves and, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) as representatives of the following classes:

Genworth Nationwide Class: All persons whose PII was compromised in the MOVEit Data Breach where such PII was obtained from or hosted by Genworth.

Genworth California Class: All residents of California whose PII was compromised in the MOVEit Data Breach where such PII was obtained from or hosted by Genworth.

Genworth Florida Class: All residents of Florida whose PII was compromised in the MOVEit Data Breach where such PII was obtained from or hosted by Genworth.

Genworth New York Class: All residents of New York whose PII was compromised in the MOVEit Data Breach where such PII was obtained from or hosted by Genworth.

Genworth Texas Class: All residents of Texas whose PII was compromised in the MOVEit Data Breach where such PII was obtained from or hosted by Genworth.

The foregoing state-specific Genworth classes are collectively referred to as the "Genworth State Classes."

2073. Additionally, PBI Bellwether Plaintiff Soto brings this action on behalf of himself and, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) as representative of the following classes:

> MLIC Nationwide Class: All persons whose PII was compromised in the MOVEit Data Breach where such PII was obtained from or hosted by MLIC.
>
> > MLIC Florida Class: All residents of Florida whose PII was compromised in the MOVEit Data Breach where such PII was obtained from or hosted by MLIC.
>
> Milliman Nationwide Class: All persons whose PII was compromised in the MOVEit Data Breach where such PII was obtained from or hosted by Milliman.
>
> > Milliman Florida Class: All residents of Florida whose PII was compromised in the MOVEit Data Breach where such PII was obtained from or hosted by Milliman.

2074. Additionally, PBI Bellwether Plaintiffs Checchia, Phelan, Uhrich, Teppler, and Marshall (collectively, "TIAA Plaintiffs") bring this action on behalf of themselves and, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) as representatives of the following classes:

> TIAA Nationwide Class: All persons whose PII was compromised in the MOVEit Data Breach where such PII was obtained from or hosted by TIAA.
>
> > TIAA Florida Class: All residents of Florida whose PII was compromised in the MOVEit Data Breach where such PII was obtained from or hosted by TIAA.
> >
> > TIAA Illinois Class: All residents of Illinois whose PII was compromised in the MOVEit Data Breach where such PII was obtained from or hosted by TIAA.
> >
> > TIAA New Jersey Class: All residents of New Jersey whose PII was compromised in the MOVEit Data Breach where such PII was obtained from or hosted by TIAA.
> >
> > TIAA Pennsylvania Class: All residents of Pennsylvania whose PII was compromised in the MOVEit Data Breach where such PII was obtained from or hosted by TIAA.

> TIAA Vermont Class: All residents of Vermont whose PII was compromised in the MOVEit Data Breach where such PII was obtained from or hosted by TIAA.

The foregoing state-specific TIAA classes are collectively referred to as the "TIAA State Classes."

2075. All of the foregoing classes are referred to in this Chapter, collectively, as the "PBI Bellwether Class." The Nationwide PBI, Genworth, MLIC, Milliman and TIAA Classes are collectively referred to as the "PBI Bellwether Nationwide Classes." The PBI State Classes, Genworth State Classes, TIAA State Classes, MLIC Florida Class, and Milliman Florida Class (i.e., all state classes alleged in the PBI Chapter) are collectively referred to as the "PBI State Classes."

2076. Excluded from the Class are: (1) the judges presiding over the action, Class Counsel, and members of their families; (2) the Defendants, their subsidiaries, parent companies, successors, predecessors, and any entity in which Defendants or their parents have a controlling interest, and their current or former officers and directors; (3) persons who properly opt out; and (4) the successors or assigns of any such excluded persons.

2077. **Numerosity**: PBI Bellwether Class Members are so numerous that their individual joinder is impracticable, as the proposed Class includes at least 40 million members who are geographically dispersed.[646]

2078. **Typicality**: PBI Bellwether Plaintiffs' claims are typical of PBI Bellwether Class Members' claims. PBI Bellwether Plaintiffs and all PBI Bellwether Class Members were injured through PBI Bellwether Defendants' uniform misconduct, and PBI Bellwether Plaintiffs' claims are identical to the claims of the PBI Bellwether Class Members they seek to represent.

---

[646] *PBI Data Breach: What & How It Happened?*, Twingate (June 14, 2024), https://www.twingate.com/blog/tips/pbi-data-breach.

2079. **Adequacy**: PBI Bellwether Plaintiffs' interests are aligned with the PBI Bellwether Class Members they seek to represent, and PBI Bellwether Plaintiffs have retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. PBI Bellwether Plaintiffs and their counsel intend to prosecute this action vigorously. The PBI Bellwether Class's interests are well-represented by PBI Bellwether Plaintiffs and undersigned counsel.

2080. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' claims. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class Members individually to effectively redress PBI Bellwether Defendants' wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

2081. **Commonality and Predominance:** The following questions common to all Class Members predominate over any potential questions affecting individual Class Members:

a. Whether PBI Bellwether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII from unauthorized access and disclosure;

b. Whether PBI Bellwether Defendants failed to exercise reasonable care to secure and safeguard PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII;

c. Whether PBI Bellwether Defendants breached their duties to protect PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII;

d. Whether PBI Bellwether Defendants violated the statutes alleged herein;

e. Whether PBI Bellwether Plaintiffs and all other PBI Bellwether Class Members are entitled to damages and the measure of such damages and relief.

2082. Given that the PBI Bellwether Defendants engaged in a common course of conduct as to PBI Bellwether Plaintiffs and PBI Bellwether Class Members, similar or identical injuries and common law violations are involved, and common questions outweigh any potential individual questions.

IV. PBI BELLWETHER CAUSES OF ACTION

PBI BELLWETHER FIRST CLAIM FOR RELIEF
Negligence
(Brought on behalf of the PBI Bellwether Nationwide Classes or, in the alternative, the PBI Bellwether State Classes)

2083. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2084. PBI Bellwether Plaintiffs bring this claim against PBI on behalf of the PBI Nationwide Class or, in the alternative, the PBI State Classes. In addition, PBI Bellwether Plaintiffs Bailey, Camille Burgan, Eugene Burgan, Gilbert Hale, Lynda Hale, Harris, Hauser, Hernandez, and Pasquarelli bring this claim against Genworth on behalf of the Genworth Nationwide Class or, in the alternative, the Genworth State Classes. PBI Bellwether Plaintiffs Checchia, Marshall, Phelan, Teppler, and Uhrich bring this claim against TIAA on behalf of the TIAA Nationwide Class or, in the alternative, the TIAA State Classes. PBI Bellwether Plaintiff Soto brings this claim against MLIC on behalf of the MLIC Nationwide Class or, in the alternative, the MLIC Florida

Class, and against Milliman on behalf of the Milliman Nationwide Class or, in the alternative, the Milliman Florida Class.

2085. PBI Bellwether Defendants owed non-delegable duties to PBI Bellwether Plaintiffs and all other PBI Bellwether Class Members to exercise reasonable care in safeguarding and protecting their PII in PBI Bellwether Defendants' possession, custody, or control, including non-delegable duties to safeguard that PII.

2086. In addition to those duties, Genworth Defendants, Milliman Defendants, MLIC, and TIAA each had additional, independent, non-delegable duties to audit, monitor, control, and/or otherwise secure all environments into which they placed PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII, and to ensure that those environments were used, configured, monitored, and/or otherwise maintained in such a way as to ensure the security and safety of PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII. Specifically, as alleged in greater detail, in the ordinary course of their business: (a) TIAA provided approximately 2.3-2.6 million individuals' highly sensitive PII to PBI; (b) Genworth Defendants provided approximately 2.5-2.7 million individuals' highly sensitive PII to PBI; (c) Milliman Defendants provided 1.28-1.325 million individuals' highly sensitive PII to PBI; and (d) MLIC provided approximately 1 million individuals' highly sensitive PII to PBI. By doing so, PBI-Contracting Defendants had non-delegable duties to PBI Bellwether Plaintiffs and PBI Bellwether Class Members to ensure that the millions of pieces of their highly sensitive PII that PBI-Contracting Defendants transmitted to PBI would remain secure. PBI-Contracting Defendants could not delegate those independent duties to their vendors and/or business associates, such as PBI or Progress.

2087. Thus, every PBI Bellwether Defendant owed independent, non-delegable duties to PBI Bellwether Plaintiffs and PBI Bellwether Class Members to exercise reasonable care in

obtaining, securing, safeguarding, storing, and protecting their PII within PBI Bellwether Defendants' control from being compromised, lost, stolen, accessed, and/or misused by unauthorized persons such as Cl0P. Further, every PBI Bellwether Defendant owed independent, non-delegable duties of care to provide security consistent with industry standards and best practices to ensure the safety and security of PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII.

2088. PBI Bellwether Defendants knew—or should have known—the risks of collecting, storing, transmitting, and/or otherwise maintaining PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII and the importance of maintaining adequate security processes and ensuring their vendors and business associates with whom PBI Bellwether Defendants shared consumers' PII—such as PBI itself and Progress—had secure services, processes, and/or procedures in place to safeguard that PII. Indeed, as alleged in greater detail, each PBI-Contracting Defendant transferred PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII compromised in the Data Breach to PBI using the MOVEit Transfer tool, such that PBI-Contracting Defendants had an opportunity to directly inspect the MOVEit Transfer tool and discover the vulnerability(ies) contained therein that led to the Data Breach, yet they failed to do so. Further, PBI Bellwether Defendants knew of the many data breaches that targeted information such as PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII, especially Social Security numbers, in recent years.

2089. Given the nature of PBI Bellwether Defendants' businesses, the sensitivity and value of the millions of individuals' PII they collect, store, transmit, and/or otherwise maintain in the ordinary course of their businesses (and the vast resources at PBI Bellwether Defendants'

disposal), PBI Bellwether Defendants should have taken steps to prevent the Data Breach from occurring.

2090. PBI Bellwether Defendants breached their non-delegable duties in numerous ways including (but not limited to) by:

a. Failing to exercise reasonable care and to implement adequate security systems, protocols, and practices sufficient to protect PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII;

b. Failing to comply with applicable industry standards and best practices regarding data security during the period of the Data Breach;

c. Failing to comply with regulations protecting the PII at issue during the period of the Data Breach;

d. Failing to recognize in a timely manner that PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII had been compromised; and

e. Failing to timely and adequately disclose that PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII had been improperly acquired or accessed.

In addition to subparts (a) – (e) above, PBI-Contracting Defendants further breached the following non-delegable duties that they each owed to PBI Bellwether Plaintiffs and PBI Bellwether Class Members:

a. Failing to adequately monitor and audit the data security systems of their vendor/business associate, PBI, and its use of the MOVEit service;

b. Failing to adequately monitor and audit the MOVEit Transfer tool when they used it in the ordinary course of their businesses, including, but not limited to, when they transferred PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII to PBI; and

c. Failing to adequately monitor, evaluate, and ensure the security of PBI's network and systems.

2091. It was reasonably foreseeable to PBI Bellwether Defendants that their failure to exercise reasonable care in safeguarding and protecting PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII—including PBI-Contracting Defendants' failure to adequately

monitor and audit PBI's systems and use of the MOVEit service—would result in the Data Breach and unauthorized release, disclosure, and dissemination of PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII to unauthorized individuals.

2092. But for PBI Bellwether Defendants' negligent conduct and breach of the above-described duties owed to PBI Bellwether Plaintiffs and PBI Bellwether Class Members, the Data Breach would not have occurred, and their PII would not have been compromised thereby. Therefore, PBI Bellwether Defendants' breaches of their duties directly and proximately caused PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' harm and damages.

2093. As a direct and proximate result of PBI Bellwether Defendants' above-described wrongful actions, inactions, and want of ordinary care that directly and proximately caused the Data Breach, PBI Bellwether Plaintiffs and PBI Bellwether Class Members have suffered, and will continue to suffer, economic damages and other injuries and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—a risk that justifies expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost value of the unauthorized access to their PII permitted by PBI Bellwether Defendants; (vi) the value of long-term credit monitoring and identity theft protection products necessitated by the Data Breach; and/or (vii) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

PBI BELLWETHER SECOND CLAIM FOR RELIEF
Negligence Per Se
(Brought on behalf of the PBI Bellwether Nationwide Classes or, in the alternative, the PBI Bellwether State Classes)

2094. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2095. PBI Bellwether Plaintiffs bring this claim against PBI on behalf of the PBI Nationwide Class or, in the alternative, the PBI State Classes. In addition, PBI Bellwether Plaintiffs Bailey, Camille Burgan, Eugene Burgan, Gilbert Hale, Lynda Hale, Harris, Hauser, Hernandez, and Pasquarelli bring this claim against Genworth on behalf of the Genworth Nationwide Class or, in the alternative, the Genworth State Classes. Plaintiffs Checchia, Marshall, Phelan, Teppler, and Uhrich bring this claim against TIAA on behalf of the TIAA Nationwide Class or, in the alternative, the TIAA State Classes. Plaintiff Soto brings this claim against MLIC on behalf of the MLIC Nationwide Class or, in the alternative, the MLIC Florida Class, and against Milliman on behalf of the Milliman Nationwide Class or, in the alternative, the Milliman Florida Class.

2096. PBI Bellwether Defendants' duties arise from, *inter alia*, Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as PBI Bellwether Defendants, of failing to employ reasonable measures to protect and secure PII.

2097. PBI Bellwether Defendants violated Section 5 of the FTCA by failing to use reasonable measures to protect PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII and not complying with applicable industry standards. PBI Bellwether Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtain and store, and the

foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to PBI Bellwether Plaintiffs and PBI Bellwether Class Members.

2098. Furthermore, Genworth Defendants, Milliman Defendants, MLIC, and TIAA have additional duties arising from, *inter alia*, the Gramm-Leach-Bliley Act (defined as "GLBA"), including duties to protect PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII by:

a. ensuring the security and confidentiality of customer records and information;

b. protecting against any anticipated threats or hazards to the security or integrity of such records; and

c. protecting against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

15 U.S.C. § 6801(b).

2099. In order to satisfy their obligations under the GLBA, Genworth Defendants, Milliman Defendants, MLIC, and TIAA were also required to "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." *See* 16 C.F.R. § 314.4.

2100. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Genworth Defendants, Milliman Defendants, MLIC, and TIAA had affirmative duties to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See id*.

2101. Further, when Genworth Defendants, Milliman Defendants, MLIC, and TIAA became aware of "unauthorized access to sensitive customer information," they had a duty to

promptly "conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused" and "notify the affected customer[s] as soon as possible." *See id*.

2102. Genworth Defendants, Milliman Defendants, MLIC, and TIAA violated the GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, Genworth Defendants', Milliman Defendants', MLIC's, and TIAA's (a) failure to implement and maintain adequate data security practices to safeguard PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII; (b) failing to detect the Data Breach in a timely manner; and (c) Genworth Defendants', Milliman Defendants', MLIC's, and TIAA's failure to disclose that their data security practices were inadequate to safeguard PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII.

2103. Genworth Defendants, Milliman Defendants, MLIC, and TIAA also violated the GLBA by failing to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." This includes, but is not limited to, Genworth Defendants', Milliman Defendants', MLIC's, and TIAA's failure to notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the Data Breach in a timely and adequate manner.

2104. Genworth Defendants, Milliman Defendants, MLIC, and TIAA also violated the GLBA by failing to notify affected customers as soon as possible after they became aware of unauthorized access to sensitive customer information.

2105. PBI Bellwether Plaintiffs and PBI Bellwether Class Members were foreseeable victims of Genworth Defendants', Milliman Defendants', MLIC's, and TIAA's violations of the GLBA. Genworth Defendants, Milliman Defendants, MLIC, and TIAA knew or should have known that their failure to take reasonable measures to prevent a breach of their data security systems—and/or that of their vendors such as PBI—and failure to timely and adequately notify the appropriate regulatory authorities, law enforcement, and PBI Bellwether Class Members themselves would cause damages to PBI Bellwether Class Members.

2106. PBI Bellwether Defendants' violations of Section 5 of the FTCA and Genworth Defendants', Milliman Defendants', MLIC's, and TIAA's violations of the GLBA constitute negligence per se.

2107. PBI Bellwether Plaintiffs and PBI Bellwether Class Members are within the class of persons that Section 5 of the FTCA and the GLBA were intended to protect.

2108. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA and the GLBA were intended to guard against.

2109. It was reasonably foreseeable to PBI Bellwether Defendants that their failure to exercise reasonable care in safeguarding and protecting PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII—including Genworth Defendants', Milliman Defendants', MLIC's, and TIAA's failure to adequately monitor and audit PBI's systems and use of the MOVEit service—would result in the Data Breach and unauthorized release, disclosure, and dissemination of PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII to unauthorized individuals.

2110. The injury and harm that PBI Bellwether Plaintiffs and PBI Bellwether Class Members suffered was the direct and proximate result of PBI Bellwether Defendants' violations of Section 5 of the FTCA and Genworth Defendants', Milliman Defendants', MLIC's, and TIAA's

violations of the GLBA. PBI Bellwether Plaintiffs and PBI Bellwether Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—a risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

PBI BELLWETHER THIRD CLAIM FOR RELIEF
Invasion of Privacy (Intrusion Upon Seclusion)
(Brought on behalf of the PBI Bellwether Nationwide Classes or, in the alternative, the PBI Bellwether State Classes)

2111. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2112. All PBI Bellwether Plaintiffs bring this claim against PBI on behalf of the PBI Nationwide Class or, in the alternative, the PBI State Classes. In addition, PBI Bellwether Plaintiffs Bailey, Camille Burgan, Eugene Burgan, Gilbert Hale, Lynda Hale, Harris, Hauser, Hernandez, and Pasquarelli bring this claim against Genworth on behalf of the Genworth Nationwide Class or, in the alternative, the Genworth State Classes. Plaintiffs Checchia, Marshall, Phelan, Teppler, and Uhrich bring this claim against TIAA on behalf of the TIAA Nationwide Class or, in the alternative, the TIAA State Classes. Plaintiff Soto brings this claim against MLIC on behalf of the MLIC Nationwide Class or, in the alternative, the MLIC Florida Class, and against Milliman on behalf of the Milliman Nationwide Class or, in the alternative, the Milliman Florida Class.

2113. PBI Bellwether Plaintiffs and PBI Bellwether Class Members had a reasonable expectation of privacy in the PII that PBI Bellwether Defendants failed to safeguard and allowed to be accessed by way of the Data Breach.

2114. PBI Bellwether Defendants' conduct as alleged intruded upon PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' seclusion under common law.

2115. By intentionally and/or knowingly failing to keep PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, PBI Bellwether Defendants intentionally invaded PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' privacy by:

a. Intentionally and substantially intruding into PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' private affairs in a manner that identifies PBI Bellwether Plaintiffs and PBI Bellwether Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about PBI Bellwether Plaintiffs and PBI Bellwether Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to PBI Bellwether Plaintiffs and PBI Bellwether Class Members.

2116. PBI Bellwether Defendants knew that an ordinary person in PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' positions would consider PBI Bellwether Defendants' intentional actions highly offensive and objectionable.

2117. PBI Bellwether Defendants invaded PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' right to privacy and intruded into PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' seclusion by intentionally failing to safeguard, misusing, and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

2118. PBI Bellwether Defendants intentionally concealed from PBI Bellwether Plaintiffs and PBI Bellwether Class Members an incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

2119. As a proximate result of such intentional misuse and disclosures, PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. PBI Bellwether Defendants' conduct, amounting to a substantial and serious invasion of PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' protected privacy interests caused anguish and suffering such that an ordinary person would consider PBI Bellwether Defendants' intentional actions or inaction highly offensive and objectionable.

2120. In failing to protect PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII, and in intentionally misusing and/or disclosing their PII, PBI Bellwether Defendants acted with intentional malice and oppression and in conscious disregard of PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' rights to have such information kept confidential and private.

2121. As a direct and proximate result of the foregoing conduct, PBI Bellwether Plaintiffs seek an award of damages on behalf of themselves and the Class Members.

PBI BELLWETHER FOURTH CLAIM FOR RELIEF
Invasion of Privacy (Public Disclosure of Private Facts)
(Brought on behalf of the PBI Bellwether Nationwide Classes or, in the alternative, the PBI Bellwether State Classes)

2122. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2123. All PBI Bellwether Plaintiffs bring this claim against PBI on behalf of the PBI Nationwide Class or, in the alternative, the PBI State Classes. In addition, PBI Bellwether Plaintiffs Bailey, Camille Burgan, Eugene Burgan, Gilbert Hale, Lynda Hale, Harris, Hauser, Hernandez,

and Pasquarelli bring this claim against Genworth on behalf of the Genworth Nationwide Class or, in the alternative, the Genworth State Classes. Plaintiffs Checchia, Marshall, Phelan, Teppler, and Uhrich bring this claim against TIAA on behalf of the TIAA Nationwide Class or, in the alternative, the TIAA State Classes. Plaintiff Soto brings this claim against MLIC on behalf of the MLIC Nationwide Class or, in the alternative, the MLIC Florida Class, and against Milliman on behalf of the Milliman Nationwide Class or, in the alternative, the Milliman Florida Class.

2124. PBI Bellwether Plaintiffs and PBI Bellwether Class Members had a reasonable expectation of privacy in the PII that they provided to PBI Bellwether Defendants, directly or indirectly, in exchange for PBI Bellwether Defendants' services, which PBI Bellwether Defendants mishandled and allowed to be comprised in the Data Breach.

2125. As a result of PBI Bellwether Defendants' conduct, publicity was given to PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII, which necessarily includes matters concerning their private life.

2126. A reasonable person of ordinary sensibilities would consider the publication of PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII to be highly offensive.

2127. PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII is not of legitimate public concern and should remain private.

2128. As a direct and proximate result of PBI Bellwether Defendants' public disclosure of private facts, PBI Bellwether Plaintiffs and PBI Bellwether Class members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to

actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their PII; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their PII, which remains in PBI Bellwether Defendants' possession, and which is subject to further breaches, so long as PBI Bellwether Defendants fail to undertake appropriate and adequate measures to protect PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII.

2129. PBI Bellwether Plaintiffs and PBI Bellwether Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

2130. PBI Bellwether Plaintiffs and PBI Bellwether Class Members are also entitled to injunctive relief requiring PBI Bellwether Defendants to, inter alia: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

PBI BELLWETHER FIFTH CLAIM FOR RELIEF
Breach of Implied Contract
(Brought on behalf of the PBI Bellwether Nationwide Classes or, in the alternative, the PBI Bellwether State Classes)

2131. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2132. PBI Bellwether Plaintiffs Bailey, Camille Burgan, Eugene Burgan, Gilbert Hale, Lynda Hale, Harris, Hauser, Hernandez, and Pasquarelli bring this claim against Genworth bring this claim against Genworth on behalf of the Genworth Nationwide Class or, in the alternative, the Genworth State Classes. Plaintiffs Checchia, Marshall, Phelan, Teppler, and Uhrich bring this claim against TIAA on behalf of the TIAA Nationwide Class or, in the alternative, the TIAA State

Classes. Plaintiff Soto brings this claim against MLIC on behalf of the MLIC Nationwide Class or, in the alternative, the MLIC Florida Class, and against Milliman on behalf of the Milliman Nationwide Class or, in the alternative, the Milliman Florida Class.

2133. Genworth Defendants, Milliman Defendants, TIAA, and MLIC (collectively, "PBI-VCE/VCEC Defendants") required PBI Bellwether Plaintiffs and PBI Bellwether Class Members to entrust them with their PII, directly or indirectly, in connection with PBI-VCE/VCEC Defendants' provision of services to PBI Bellwether Plaintiffs and PBI Bellwether Class Members.

2134. In turn, and through internal policies set forth herein, PBI-VCE/VCEC Defendants agreed to safeguard and not disclose to unauthorized persons the PII they collected from PBI Bellwether Plaintiffs and PBI Bellwether Class Members, directly or indirectly.

2135. PBI Bellwether Plaintiffs and PBI Bellwether Class Members accepted PBI-VCE/VCEC Defendants' offers by providing PII to them—either directly or through certain Bellwether Defendants—in exchange for PBI-VCE/VCEC Defendants' services.

2136. Implicit in the parties' agreement was that PBI-VCE/VCEC Defendants would adequately safeguard the PII entrusted to them and would provide PBI Bellwether Plaintiffs and PBI Bellwether Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

2137. PBI Bellwether Plaintiffs and PBI Bellwether Class Members would not have entrusted their PII to PBI-VCE/VCEC Defendants in the absence of such an agreement.

2138. PBI-VCE/VCEC Defendants materially breached the contract(s) they had entered into with PBI Bellwether Plaintiffs and PBI Bellwether Class Members by failing to safeguard such PII and failing to notify them promptly of the intrusion into their computer systems that

compromised such information. PBI-VCE/VCEC Defendants further breached the implied contracts with PBI Bellwether Plaintiffs and PBI Bellwether Class Members by:

a. Failing to properly safeguard and protect PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that PBI-VCE/VCEC Defendants created, received, maintained, and transmitted.

2139. The damages sustained by PBI Bellwether Plaintiffs and PBI Bellwether Class Members as described above were the direct and proximate result of PBI-VCE/VCEC Defendants' material breaches of their implied agreement(s).

2140. PBI Bellwether Plaintiffs and PBI Bellwether Class Members have performed as required under the relevant agreements, or such performance was waived by the conduct of PBI-VCE/VCEC Defendants.

2141. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

2142. Subterfuge and evasion—such as that of PBI-VCE/VCEC Defendants, as alleged in greater detail herein—violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

2143. PBI-VCE/VCEC Defendants knew or should have known that PBI Bellwether Plaintiffs and PBI Bellwether Class Members reasonably understood that PBI Bellwether Defendants would safeguard the PII that PBI-VCE/VCEC Defendants required PBI Bellwether Plaintiffs and PBI Bellwether Class Members to disclose in order to provide PBI-VCE/VCEC Defendants' services to them. Despite PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' reasonable expectations, PBI-VCE/VCEC Defendants failed to implement appropriate cybersecurity protocols to protect the PII on their systems from the Data Breach.

2144. In addition, PBI-VCE/VCEC Defendants failed to advise PBI Bellwether Plaintiffs and PBI Bellwether Class Members of the Data Breach promptly and sufficiently. PBI-VCE/VCEC Defendants' own websites and other statements promised PBI Bellwether Plaintiffs and PBI Bellwether Class Members that PBI-VCE/VCEC Defendants would keep their PII safe and promptly notify them of any data breaches. PBI-VCE/VCEC Defendants, however, failed to do so, having waited multiple months before notifying PBI Bellwether Plaintiffs and PBI Bellwether Class Members of the Data Breach.

2145. In these and other ways, PBI-VCE/VCEC Defendants violated their duties of good faith and fair dealing.

2146. PBI Bellwether Plaintiffs and PBI Bellwether Class Members have sustained injury and damages because of PBI-VCE/VCEC Defendants' breaches of their agreements, including breaches thereof through violations of the covenant of good faith and fair dealing, including, without limitation: unauthorized disclosure of their PII and publication onto the Dark Web; monetary losses; lost time; anxiety, and emotional distress; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; out-of-pocket costs associated with the prevention, detection, recovery, and remediation from

identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; unauthorized use of stolen PII; continued risk to their PII, which remains in PBI Bellwether Defendants' possession and is subject to further breaches so long as PBI Bellwether Defendants fail to undertake the appropriate measures to protect the PII in their possession; increased risk of harm; and lost benefit of the bargain.

PBI BELLWETHER SIXTH CLAIM FOR RELIEF
Breach of Third-Party Beneficiary Contract
(Brought on behalf of the PBI Bellwether Nationwide Classes or, in the alternative, the PBI Bellwether State Classes)

2147. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2148. PBI Bellwether Plaintiffs Bailey, Camille Burgan, Eugene Burgan, Gilbert Hale, Lynda Hale, Harris, Hauser, Hernandez, and Pasquarelli bring this claim against Genworth bring this claim against Genworth on behalf of the Genworth Nationwide Class or, in the alternative, the Genworth State Classes. Plaintiffs Checchia, Marshall, Phelan, Teppler, and Uhrich bring this claim against TIAA on behalf of the TIAA Nationwide Class or, in the alternative, the TIAA State Classes. Plaintiff Soto brings this claim against MLIC on behalf of the MLIC Nationwide Class or, in the alternative, the MLIC Florida Class, and against Milliman on behalf of the Milliman Nationwide Class or, in the alternative, the Milliman Florida Class.

2149. PBI Bellwether Defendants entered into contracts with their government and corporate customers to provide services to them using MOVEit; services that included data

security practices, procedures, and protocols sufficient to safeguard the PII that was entrusted to PBI Bellwether Defendants. Those contracts entered into by PBI Bellwether Defendants were made expressly for the benefit of PBI Bellwether Plaintiffs and PBI Bellwether Class Members—namely to provide services that kept their PII secure—as it was their PII that PBI Bellwether Defendants agreed to receive, store, utilize, transfer, and protect through their services. Thus, the benefit of collection and protection of the PII belonging to PBI Bellwether Plaintiffs and PBI Bellwether Class Members was the direct and primary objective of the contracting parties and PBI Bellwether Plaintiffs and PBI Bellwether Class Members were direct and express beneficiaries of such contracts.

2150. PBI Bellwether Defendants knew or should have known that if they were to breach these contracts, PBI Bellwether Plaintiffs and PBI Bellwether Class Members would be harmed.

2151. PBI Bellwether Defendants breached their contracts by, among other things, failing to adequately secure PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII, and, as a result, PBI Bellwether Plaintiffs and PBI Bellwether Class Members were harmed by PBI Bellwether Defendants' failure to secure their PII.

2152. As a direct and proximate result of PBI Bellwether Defendants' breach, PBI Bellwether Plaintiffs and PBI Bellwether Class Members are at a current and ongoing risk of identity theft, and PBI Bellwether Plaintiffs and PBI Bellwether Class Members sustained incidental and consequential damages including: (i) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out of pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails;

(vi) diminution of value of their PII; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their PII, which remains in PBI Bellwether Defendants' control, and which is subject to further breaches, so long as PBI Bellwether Defendants fail to undertake appropriate and adequate measures to protect PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII.

2153. PBI Bellwether Plaintiffs and PBI Bellwether Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

2154. PBI Bellwether Plaintiffs and PBI Bellwether Class Members are also entitled to injunctive relief requiring PBI Bellwether Defendants to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

PBI BELLWETHER SEVENTH CLAIM FOR RELIEF|
Unjust Enrichment
(Brought on behalf of the PBI Bellwether Nationwide Classes or, in the alternative, the PBI Bellwether State Classes)

2155. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2156. PBI Bellwether Plaintiffs bring this claim against PBI on behalf of the PBI Nationwide Class or, in the alternative, the PBI State Classes. In addition, PBI Bellwether Plaintiffs Bailey, Camille Burgan, Eugene Burgan, Gilbert Hale, Lynda Hale, Harris, Hauser, Hernandez, and Pasquarelli bring this claim against Genworth on behalf of the Genworth Nationwide Class or, in the alternative, the Genworth State Classes. Plaintiffs Checchia, Marshall, Phelan, Teppler, and Uhrich bring this claim against TIAA on behalf of the TIAA Nationwide Class or, in the alternative, the TIAA State Classes. Plaintiff Soto brings this claim against MLIC on behalf of the MLIC

Nationwide Class or, in the alternative, the MLIC Florida Class, and against Milliman on behalf of the Milliman Nationwide Class or, in the alternative, the Milliman Florida Class.

2157. PBI Bellwether Plaintiffs and PBI Bellwether Class Members have both a legal and equitable interest in their PII that was collected by, stored by, and maintained by PBI Bellwether Defendants—thus conferring a benefit upon PBI Bellwether Defendants by transmitting that PII to them or otherwise allowing them to possess it—that was ultimately compromised by the Data Breach.

2158. PBI Bellwether Defendants accepted or had knowledge of the benefits conferred upon them by PBI Bellwether Plaintiffs and PBI Bellwether Class Members by, *inter alia*, accepting or otherwise possessing PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII. PBI Bellwether Defendants also benefitted from the receipt of PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII.

2159. As a result of PBI Bellwether Defendants' failure to safeguard and protect PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII, they suffered actual damages as a result of the Data Breach. Thus, it would be unjust for PBI Bellwether Defendants to be permitted to retain the benefit belonging to PBI Bellwether Plaintiffs and PBI Bellwether Class Members because PBI Bellwether Defendants failed to adequately implement the data privacy and security procedures that were mandated by federal, state, and local laws and industry standards.

2160. PBI Bellwether Defendants should be compelled to provide for the benefit of PBI Bellwether Plaintiffs and PBI Bellwether Class Members all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

PBI BELLWETHER EIGHTH CLAIM FOR RELIEF
Violation of Massachusetts General Laws, Chapter 93A
(Brought on behalf of the PBI Bellwether Nationwide Classes or, in the alternative, the PBI Bellwether State Classes)

2161. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2162. PBI Bellwether Plaintiffs bring this claim against PBI on behalf of the PBI Nationwide Class or, in the alternative, the PBI State Classes. In addition, PBI Bellwether Plaintiffs Bailey, Camille Burgan, Eugene Burgan, Gilbert Hale, Lynda Hale, Harris, Hauser, Hernandez, and Pasquarelli bring this claim against Genworth on behalf of the Genworth Nationwide Class or, in the alternative, the Genworth State Classes. Plaintiffs Checchia, Marshall, Phelan, Teppler, and Uhrich, bring this claim against TIAA on behalf of the TIAA Nationwide Class or, in the alternative, the TIAA State Classes. Plaintiff Soto brings this claim against MLIC on behalf of the MLIC Nationwide Class or, in the alternative, the MLIC Florida Class, and against Milliman on behalf of the Milliman Nationwide Class or, in the alternative, the Milliman Florida Class.

2163. M.G.L. ch. 93A §§ 2 and 9. M.G.L. ch. 93A § 2 provides that "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." M.G.L. ch. 93A § 9 permits any consumer injured by a violation of M.G.L. ch. 93A § 2 to bring a civil action, including a class action, for damages and injunctive relief.

2164. PBI Bellwether Plaintiffs allege that PBI Bellwether Defendants committed unfair business acts and/or practices in violation of M.G.L. ch. 93A §§ 2 and 9.

2165. PBI Bellwether Defendants knew or should have known of the inherent risks in experiencing a data breach if they failed to maintain adequate systems and processes for keeping

PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII safe and secure. Only PBI Bellwether Defendants were in a position to ensure that their systems were sufficient to protect against harm to PBI Bellwether Plaintiffs and PBI Bellwether Class Members resulting from a data security incident such as the Data Breach; instead, they failed to implement such safeguards.

2166. PBI Bellwether Defendants' own conduct also created a foreseeable risk of harm to PBI Bellwether Plaintiffs and PBI Bellwether Class Members and their PII. PBI Bellwether Defendants' misconduct included failing to adopt, implement, and maintain the systems, policies, and procedures necessary to prevent the Data Breach.

2167. PBI Bellwether Defendants acknowledge their conduct created actual harm to PBI Bellwether Plaintiffs and PBI Bellwether Class Members because PBI Bellwether Defendants instructed them to monitor their accounts for fraudulent conduct and identity theft.

2168. PBI Bellwether Defendants knew, or should have known, of the risks inherent in disclosing, collecting, storing, accessing, and transmitting PII and the importance of adequate security because of, *inter alia*, the prevalence of data breaches.

2169. PBI Bellwether Defendants failed to adopt, implement, and maintain fair, reasonable, or adequate security measures to safeguard PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII, failed to recognize the Data Breach in a timely manner, and failed to notify PBI Bellwether Plaintiffs and PBI Bellwether Class Members in a timely manner that their PII was accessed in the Data Breach.

2170. These acts and practices are unfair in material respects, offend public policy, are immoral, unethical, oppressive and unscrupulous and violate 201 CMR 17.00 and M.G.L. ch. 93A § 2.

2171. As a direct and proximate result of PBI Bellwether Defendants' unfair acts and practices, PBI Bellwether Plaintiffs and PBI Bellwether Class Members have suffered injury and/or will suffer injury and damages, including, but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the publication and/or fraudulent use of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest and recover from unemployment and/or tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in PBI Bellwether Defendants' possession (and/or to which PBI Bellwether Defendants continue to have access) and is subject to further unauthorized disclosures so long as PBI Bellwether Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of disclosed PII.

2172. Neither PBI Bellwether Plaintiffs nor PBI Bellwether Class Members contributed to the Data Breach.

2173. PBI Bellwether Plaintiffs sent a demand for relief, in writing, to PBI Bellwether Defendants on or about November 6, 2024, prior to filing this complaint. Multiple plaintiffs in

consolidated actions have sent[647]—or alleged in their complaints that they would send[648]—similar demand letters as required by M.G.L. ch. 93A § 9. PBI Bellwether Plaintiffs have not received a written tender of settlement that is reasonable in relation to the injury actually suffered by PBI Bellwether Plaintiffs and PBI Bellwether Class Members.

2174. Based on the foregoing, PBI Bellwether Plaintiffs and PBI Bellwether Class Members are entitled to all remedies available pursuant to M.G.L ch. 93A, including, but not limited to, refunds, actual damages, or statutory damages in the amount of twenty-five dollars per violation, whichever is greater, double or treble damages, attorneys' fees and other reasonable costs.

2175. Pursuant to M.G.L. ch. 231, § 6B, PBI Bellwether Plaintiffs and PBI Bellwether Class Members are further entitled to pre-judgment interest as a direct and proximate result of PBI Bellwether Defendants' wrongful conduct. The amount of damages suffered as a result is a sum

[647] *See, e.g.*, *Ghalem, et al. v. Progress Software Co., et al.*, 23-cv-12300 (D. Mass.), at ECF No. 1, ¶ 213 ("A demand identifying the claimant and reasonably describing the unfair or deceptive act or practice relied upon and the injury suffered was mailed or delivered to Defendants at least thirty days prior to the filing of a pleading alleging this claim for relief").

[648] In all of the following cases (among others), plaintiffs indicated that they were going to send similar demand letters: *Allen, et al. v. Progress Software Corp.*, 23-cv-11984 (D. Mass.); *Anastasio v. Progress Software Corp., et al.*, 23-cv-11442 (D. Mass.); *Arden v. Progress Software Corp., et al.*, 23-cv-12015 (D. Mass.); *Boaden v. Progress Software Corp., et al.*, 23-cv-12192 (D. Mass.); *Brida v. Progress Software Corp., et al.*, 23-cv-12202 (D. Mass.); *Casey v. Progress Software Corp., et al.*, 23-cv-11864 (D. Mass.); *Constantine v. Progress Software Corp., et al.*, 23-cv-12836 (D. Mass.); *Daniels v. Progress Software Corp., et al.*, 23-cv-12010 (D. Mass.); *Doe v. Progress Software Corp., et al.*, 23-cv-1933 (D. Md.); *Ghalem, et al. v. Progress Software Co., et al.*, 23-cv-12300 (D. Mass.); *Kennedy v. Progress Software Corp., et al.*, 23-cv-12275 (D. Mass.); *Kurtz v. Progress Software Corp., et al.*, 23-cv-12156 (D. Mass.); *McDaniel, et al. v. Progress Software Corp., et al.*, 23-cv-11939 (D. Mass.); *Pilotti-Iulo v. Progress Software Corp., et al.*, 23-cv-12157 (D. Mass.); *Pulignani v. Progress Software Corp., et al.*, 23-cv-1912 (D. Md.); *Siflinger, et al. v. Progress Software Corp., et al.*, 23-cv-11782 (D. Mass.); *Tenner v. Progress Software Corp.*, 23-cv-11412 (D. Mass.); *Truesdale v. Progress Software Corp., et al.*, 23-cv-1913 (D. Md.).

certain and capable of calculation and PBI Bellwether Plaintiffs and PBI Bellwether Class Members are entitled to interest in an amount according to proof.

PBI BELLWETHER NINTH CLAIM FOR RELIEF
Violation of Minnesota Consumer Fraud Act
Minn. Stat. §§ 325F.68, *et seq*. and Minn. Stat. §§ 8.31, *et seq*.
(Brought on behalf of the PBI Bellwether Nationwide Classes or, in the alternative, the PBI Bellwether State Classes)

2176. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2177. PBI Bellwether Plaintiffs bring this claim against PBI on behalf of the PBI Nationwide Class or, in the alternative, the PBI State Classes. In addition, PBI Bellwether Plaintiffs Bailey, Camille Burgan, Eugene Burgan, Gilbert Hale, Lynda Hale, Harris, Hauser, Hernandez, and Pasquarelli bring this claim against Genworth on behalf of the Genworth Nationwide Class or, in the alternative, the Genworth State Classes. Plaintiffs Checchia, Marshall, Phelan, Teppler, and Uhrich, bring this claim against TIAA on behalf of the TIAA Nationwide Class or, in the alternative, the TIAA State Classes. Plaintiff Soto brings this claim against MLIC on behalf of the MLIC Nationwide Class or, in the alternative, the MLIC Florida Class, and against Milliman on behalf of the Milliman Nationwide Class or, in the alternative, the Milliman Florida Class.

2178. PBI Bellwether Defendants, PBI Bellwether Plaintiffs, and PBI Bellwether Class Members are each a "person" as defined by Minn. Stat. § 325F.68(3).

2179. PBI Bellwether Defendants' goods, services, commodities, and intangibles are "merchandise" as defined by Minn. Stat. § 325F.68(2).

2180. PBI Bellwether Defendants engaged in "sales" as defined by Minn. Stat. § 325F.68(4).

2181. PBI Bellwether Defendants engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in connection with the sale of merchandise, in violation of Minn. Stat. § 325F.69(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect PBI Bellwether Plaintiffs' and Class Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of PBI Bellwether Plaintiffs' and Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of PBI Bellwether Plaintiffs' and Class Members' PII, including by implementing and maintaining reasonable security measures and ensuring their vendors and business associates maintained reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of PBI Bellwether Plaintiffs' and Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure PBI Bellwether Plaintiffs' and Class Members' PII or ensure their vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of PBI Bellwether Plaintiffs' and Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45.

2182. PBI Bellwether Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of their data security and ability to protect the confidentiality of consumers' PII.

2183. PBI Bellwether Defendants intended to mislead PBI Bellwether Plaintiffs and Class Members and induce them to rely on their misrepresentations and omissions.

2184. PBI Bellwether Defendants' fraudulent, misleading, and deceptive practices affected the public interest, including those affected by the Data Breach.

2185. As a direct and proximate result of PBI Bellwether Defendants' fraudulent, misleading, and deceptive practices, PBI Bellwether Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

2186. PBI Bellwether Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including damages; injunctive or other equitable relief; and attorneys' fees, disbursements, and costs.

PBI BELLWETHER TENTH CLAIM FOR RELIEF
Violation of Minnesota Uniform Deceptive Trade Practices Act
Minn. Stat. §§ 325D.43, *et seq*.
(Brought on behalf of the PBI Bellwether Nationwide Classes or, in the alternative, the PBI Bellwether State Classes)

2187. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2188. PBI Bellwether Plaintiffs bring this claim against PBI on behalf of the PBI Nationwide Class or, in the alternative, the PBI State Classes. In addition, PBI Bellwether Plaintiffs Bailey, Camille Burgan, Eugene Burgan, Gilbert Hale, Lynda Hale, Harris, Hauser, Hernandez,

and Pasquarelli bring this claim against Genworth on behalf of the Genworth Nationwide Class or, in the alternative, the Genworth State Classes. Plaintiffs Checchia, Marshall, Phelan, Teppler, and Uhrich, bring this claim against TIAA on behalf of the TIAA Nationwide Class or, in the alternative, the TIAA State Classes. Plaintiff Soto brings this claim against MLIC on behalf of the MLIC Nationwide Class or, in the alternative, the MLIC Florida Class, and against Milliman on behalf of the Milliman Nationwide Class or, in the alternative, the Milliman Florida Class.

2189. By engaging in deceptive trade practices in the course of their businesses and vocations, directly or indirectly affecting the people of Minnesota, PBI Bellwether Defendants violated Minn. Stat. § 325D.44, including the following provisions:

a. Representing that their goods and services had characteristics, uses, and benefits that they did not have, in violation of Minn. Stat. § 325D.44(1)(5);

b. Representing that goods and services are of a particular standard or quality when they are of another, in violation of Minn. Stat. § 325D.44(1)(7);

c. Advertising goods and services with intent not to sell them as advertised, in violation of Minn. Stat. § 325D.44(1)(9); and

d. Engaging in other conduct which similarly creates a likelihood of confusion or misunderstanding, in violation of Minn. Stat. § 325D.44(1)(13).

2190. PBI Bellwether Defendants' deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect PBI Bellwether Plaintiffs' and Class Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of PBI Bellwether Plaintiffs' and Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of PBI Bellwether Plaintiffs' and Class Members' PII, including by implementing and maintaining reasonable security measures and ensuring their vendors and business associates maintained reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of PBI Bellwether Plaintiffs' and Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure PBI Bellwether Plaintiffs' and Class Members' PII or ensure their vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of PBI Bellwether Plaintiffs' and Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45.

2191. PBI Bellwether Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of their data security and ability to protect the confidentiality of consumers' PII.

2192. PBI Bellwether Defendants intended to mislead PBI Bellwether Plaintiffs and Class Members and induce them to rely on their misrepresentations and omissions.

2193. Had PBI Bellwether Defendants disclosed to PBI Bellwether Plaintiffs and Class Members that their data systems were not secure and, thus, vulnerable to attack, PBI Bellwether Defendants would have been unable to continue in business and they would have been forced to use vendors and business associates with reasonable data security measures and comply with the law. Instead, PBI Bellwether Defendants received, maintained, and compiled PBI Bellwether Plaintiffs' and Class Members' PII as part of the services they provided without advising PBI Bellwether Plaintiffs and Class Members that PBI Bellwether Defendants' data security practices were insufficient to maintain the safety and confidentiality of PBI Bellwether Plaintiffs' and Class

Members' PII. Accordingly, PBI Bellwether Plaintiffs and Class Members acted reasonably in relying on PBI Bellwether Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

2194. PBI Bellwether Defendants acted intentionally, knowingly, and maliciously to violate Minnesota's Uniform Deceptive Trade Practices Act, and recklessly disregarded PBI Bellwether Plaintiffs' and Class Members' rights. PBI Bellwether Defendants' past data breaches and/or knowledge of past data breaches in their respective industries put them on notice that their security and privacy protections were inadequate and/or susceptible to being targeted for a data breach.

2195. As a direct and proximate result of PBI Bellwether Defendants' deceptive trade practices, PBI Bellwether Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

2196. PBI Bellwether Plaintiffs and Class Members seek all relief allowed by law, including injunctive relief and reasonable attorneys' fees and costs.

PBI BELLWETHER ELEVENTH CLAIM FOR RELIEF
Violations of the California Consumer Privacy Act ("CCPA")
Cal. Civ. Code § 1798.150
(Brought on behalf of the Genworth California Class and PBI California Class)

2197. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2198. Plaintiffs Camille Burgan, Eugene Burgan, Harris, and Pasquarelli ("California PBI Plaintiffs") bring this claim against Genworth Defendants on behalf of the Genworth California Class, and PBI on behalf of the PBI California Class (the "California Classes").

2199. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA.

2200. California PBI Plaintiffs and California Classes Members are within the CCPA's definition of "consumers" (as defined in § 1798.140(g)) in that they are natural persons who are California residents.

2201. PBI and Genworth are each within the definition of "business" (as defined in § 1798.140(b)) in that they are corporations organized for profit or financial benefit of their shareholders or other owners, with gross revenue in excess of $25 million.

2202. PBI and Genworth conduct substantial business in the state of California. Genworth Defendants' business within the state of California consists of the marketing, sale, delivery, maintenance, and administration of thousands of life insurance policies, representing billions of dollars in benefits, as well as the maintenance of dozens of sales and agent offices. PBI's business within the state of California consists of the marketing, sale, delivery, maintenance, and administration of its pension benefit services to pensions and businesses in the state of California, including the state's CalPERS and CalSTRS programs with millions of pension participants. PBI provided services for Genworth's California policies.

2203. In the ordinary course of their business operations in the state of California (as alleged in the immediately preceding *supra* ¶ 372), PBI and Genworth collect PII they obtain from their customers. PBI collects PII that it receives from its customers, such as Genworth, in order to provide services, including determining whether a customer may have passed and triggered death

benefits under a life insurance policy or annuity contract. Genworth collects PII from its insureds and prospective insureds, including California residents. Thus, PBI and Genworth determine which PII to retain or transfer, where and how to store it, and how to search and process the information according to their business needs, among other decisions.

2204. PBI and Genworth determine which information to transfer, collect, or otherwise possess that information, how to store and process that information, and how to access it for their business needs, among other decisions.

2205. The PII of California PBI Plaintiffs and the California Classes at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the information Genworth and PBI collect and which was impacted by the cybersecurity attack includes "[a]n individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (i) Social security number. (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual. (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (iv) Medical information. (v) Health insurance information."

2206. Genworth and PBI violated § 1798.150 of the CCPA by failing to protect California PBI Plaintiffs' and California Classes Members' PII from unauthorized access, decryption, exfiltration, theft, and/or disclosure as a result of Genworth's and PBI's violations of their duties to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

2207. Genworth and PBI each had and have a duty to implement and maintain reasonable security procedures and practices to protect California PBI Plaintiffs' and California Classes Members' PII. As detailed herein, they failed to do so.

2208. As a direct and proximate result of Genworth's and PBI's violations of their duty, some combination of California PBI Plaintiffs' and California Classes Members' names with some combination of the following: Social Security number, date of birth, zip code, state of residence, role in policy/account (e.g., Annuitant, Joint Insured, Owner, etc.), general product type, and policy/account number, were subjected to unauthorized access and exfiltration, theft, or disclosure.

2209. As a direct and proximate result of Genworth's and PBI's acts, California PBI Plaintiffs and the California Classes were injured and lost money or property, including, but not limited to, the loss of California PBI Plaintiffs' and the California Classes Members' legally protected interest in the confidentiality and privacy of their PII, the lost benefit of the bargain, diminution of value of their PII, stress, fear, and anxiety, nominal damages, and additional losses described above.

2210. California PBI Plaintiffs and the California Classes by way of this complaint seek to recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater; actual pecuniary damages suffered as a result of Genworth's and PBI's violations described herein; and injunctive relief pursuant to § 1798.150(a)(1).

2211. California PBI Plaintiffs have issued a notice of these alleged violations pursuant to § 1798.150(b).

PBI BELLWETHER TWELFTH CLAIM FOR RELIEF
Violations of the California Customer Records Act
Cal. Civ. Code § 1798.150
(Brought on behalf of the Genworth California Class and PBI California Class)

2212. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2213. California PBI Plaintiffs bring this claim against Genworth Defendants on behalf of the Genworth California Class, and PBI on behalf of the PBI California Class.

2214. Genworth is a business that owns, maintains, and licenses personal information within the meaning of Cal. Civ. Code § 1798.80(a), about California PBI Plaintiffs and California Classes Members.

2215. PBI is a business that owns, maintains, and licenses personal information within the meaning of Cal. Civ. Code § 1798.80(a), about California PBI Plaintiffs and California Classes Members.

2216. Businesses that own or license computerized data that includes personal information are required to notify California residents when their PII has been acquired, "or is reasonably believed to have been[] acquired by an unauthorized person" in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82(a). Among other requirements, the security breach notification must include "the types of personal information that were or are reasonably believed to have been the subject of the breach" pursuant to the model security breach form provided in Cal. Civ. Code § 1798.82(d).

2217. Because PBI and Genworth reasonably believed that California PBI Plaintiffs' and California Classes Members' PII was acquired by unauthorized persons during the Data Breach,

PBI and Genworth had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

2218. PBI and Genworth failed to fully disclose material information about the Data Breach in a timely and accurate manner, thereby violating Cal. Civ. Code § 1798.82.

2219. By PBI and Genworth's waiting over two months to notify California PBI Plaintiffs and California Classes Members that their PII had been compromised, California PBI Plaintiffs and California Classes Members were prevented from taking appropriate, reasonable precautions to mitigate harms caused by the Data Breach.

2220. As a direct and proximate result of PBI's and Genworth's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, California PBI Plaintiffs and California Classes Members suffered damages, as described above.

2221. California PBI Plaintiffs and California Classes Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

PBI BELLWETHER THIRTEENTH CLAIM FOR RELIEF
Violations of the California Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code §§ 17200, *et seq*.
(Brought on behalf of the Genworth California Class and PBI California Class)

2222. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2223. California PBI Plaintiffs bring this claim against Genworth Defendants on behalf of the Genworth California Class, and PBI on behalf of the PBI California Class.

2224. PBI is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

2225. Genworth is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

2226. Cal. Bus. & Prof. Code § 17204 provides that "a person who has suffered injury in fact and has lost money or property as a result of the unfair competition" may file suit.

2227. PBI and Genworth violated Cal. Bus. & Prof. Code § 17200 *et seq*. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

2228. PBI and Genworth's "unfair" acts and practices include:

a. Failure to implement and maintain reasonable security measures to protect California PBI Plaintiffs' and California Classes Members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach, California PBI Plaintiffs' and California Classes Members' PII being compromised, and subsequent harms caused to California PBI Plaintiffs and California Classes Members.

b. Failure to identify foreseeable security risks, including in their third-party vendor, Progress, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

c. Failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTCA, 15 U.S.C. § 45; California's Consumer Records Act, Cal. Civ. Code § 1798.81.5; and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150; and

d. Failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of PBI and Genworth's inadequate security practices and policies, consumers could not have reasonably avoided the harms that PBI and Genworth caused.

2229. PBI and Genworth have also engaged in unlawful business practices by violating the California Consumer Records Act, Cal. Civ. Code § 1798.81.5, and/or the California Consumer Privacy Act, Cal. Civ. Code § 1798.150, as well as the common law.

2230. PBI and Genworth's deceptive acts and practices include:

a. Misrepresenting that they would protect the privacy and confidentiality of California PBI Plaintiffs' and California Classes Members' PII, including by implementing and maintaining reasonable security measures;

b. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of California PBI Plaintiffs' and California Classes Members' personal information, including duties imposed by the FTCA, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., California's Consumer Privacy Act, Cal. Civ. Code § 1798.150; and the common law;

c. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure California PBI Plaintiffs' and California Classes Members' PII; and

d. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of California PBI Plaintiffs' and California Classes Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, and the common law.

2231. PBI and Genworth's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of PBI and Genworth's respective data security policies and practices and ability to protect the confidentiality of consumers' personal information.

2232. Had PBI and Genworth disclosed to consumers and the public that they were not complying with industry standards or regulation or that its data systems were not secure and, thus, were vulnerable to attack, they would have been unable to continue in business and they would have been forced to adopt reasonable data security measures and comply with the law.

2233. Accordingly, California PBI Plaintiffs and California Classes Members acted reasonably in relying on PBI and Genworth's misrepresentations and omissions, the truth of which they could not have discovered.

2234. PBI and Genworth were entrusted, either directly or indirectly, with sensitive and valuable PII regarding millions of consumers, including California PBI Plaintiffs and California

Classes Members. PBI and Genworth accepted the critical responsibility of protecting the data but kept the inadequate state of its security controls secret from the public.

2235. As a direct and proximate result of PBI and Genworth's unfair, unlawful, and/or fraudulent acts and practices, California PBI Plaintiffs and California Classes Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including, but not limited to, fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Genworth's products and services; loss of the value of access to their PII; and the value of identity and credit protection and repair services made necessary by the Data Breach.

2236. PBI and Genworth's violations were, and are, willful, deceptive, unfair, and unconscionable.

2237. California PBI Plaintiffs and California Classes Members have lost money and property as a result of PBI and Genworth's conduct in violation of the UCL, as stated herein and above.

2238. By deceptively, unfairly, and unlawfully storing, collecting, and disclosing their personal information, PBI and Genworth have taken money or property from California PBI Plaintiffs and Classes Members. PBI and Genworth acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded California PBI Plaintiffs' and California Classes Members' rights.

2239. PBI and Genworth knew or should have known that their data security was insufficient to guard against cyberattacks, particularly, given the size of their databases and the sensitivity of the PII therein.

2240. California PBI Plaintiffs and California Classes Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from PBI and Genworth's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

PBI BELLWETHER FOURTEENTH CLAIM FOR RELIEF
Violation of the California Consumer Legal Remedies Act (CLRA)
Cal. Civ. Code §§ 1750, *et seq*.
(Brought on behalf of the Genworth California Class)

2241. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2242. California PBI Plaintiffs bring this claim against Genworth Defendants on behalf of the Genworth California Class.

2243. The Consumers Legal Remedies Act ("CLRA"), Cal. Civ. Code §§ 1750, *et seq*., is a comprehensive statutory scheme that is to be "liberally construed" to protect consumers against unfair and deceptive business practices by businesses providing goods or services to consumers. Cal. Civ. Code § 1760.

2244. Genworth Defendants are all within the definition of "person" set forth in Cal. Civ. Code § 1761(c).

2245. California PBI Plaintiffs and the members of the Genworth California Class are "consumers" as defined in Cal. Civ. Code § 1761(d).

2246. Genworth Defendants have provided "services" as defined in Cal. Civ. Code § 1761(b).

2247. California PBI Plaintiffs and the members of the Genworth California Class have engaged in "transactions" as defined in Civil Code § 1761(e).

2248. Cal. Civ. Code § 1770(a) states:

> (a) The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction . . . that results in the sale or lease of goods or services to any consumer are unlawful:
>
> . . . .
>
> (5) Representing that goods or services have . . . characteristics, . . . uses, [or] benefits . . . that they do not have . . . [or]
>
> . . . .
>
> (7) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another.

2249. Genworth Defendants' and PBI's acts and practices resulted in the sale of services that violated Cal. Civil Code § 1770(a)(5) and (7).

2250. Omissions are actionable under Cal. Civil Code § 1770(a)(5) and (7) such that Genworth Defendants are also liable under the CLRA for their omissions.

2251. Genworth Defendants' unlawful acts included the following:

a. Genworth omitted and concealed the fact that it did not employ reasonable safeguards to protect customers' PII. Genworth could and should have made a proper disclosure when accepting applications for insurance, during the underwriting process, when the insurance policy was issued, or by any other means reasonably calculated to inform customers of the inadequate data security. Genworth knew or should have known that Genworth's data security practices and those of Genworth's vendor, PBI, were deficient. This is true because, among other things, Genworth was aware that those in the insurance industry are frequent targets of sophisticated cyberattacks. Genworth knew or should have known that Genworth's data security was insufficient to guard against those attacks.

b. Genworth also made implied or implicit representations that Genworth's data security practices were sufficient to protect customers' PII. Genworth required customers to provide their PII when applying for insurance and when taking out a policy. In doing so, Genworth made implied or implicit representations that Genworth's data security practices were sufficient to protect customers' PII. By virtue of accepting California PBI Plaintiffs' PII

> during the application and policy issuance process, Genworth implicitly represented that Genworth's data security processes were sufficient to safeguard the PII. Those representations were false and misleading.

2252. Genworth's misrepresentations and omissions were material because they were likely to and did deceive reasonable consumers about the adequacy of Genworth's data security and ability to protect the confidentiality of consumers' PII.

2253. Had Genworth disclosed to California PBI Plaintiffs and the members of the Genworth California Class that Genworth's data systems were not reasonably secure, Genworth would have been unable to continue in business in like fashion and would have been forced to adopt reasonable data security measures. Instead, Genworth received, maintained, and compiled customers' PII as part of the services Genworth provided and for which California PBI Plaintiffs and the members of the Genworth California Class paid, without advising them that Genworth's data security practices were insufficient to protect their PII.

2254. California PBI Plaintiffs and the members of the Genworth California Class transacted with Genworth in California by, among other things, applying for and purchasing insurance products from California. California PBI Plaintiffs and the members of the Genworth California Class were deceived in California when they applied for and purchased insurance products from California and were not informed of Genworth's deficient data security practices.

2255. Cal. Civ. Code § 1780(a) states:

> Any consumer who suffers any damage as a result of the use or employment by any person of a method, act, or practice declared to be unlawful by Section 1770 may bring an action against that person to recover or obtain any of the following:
>
> (1) Actual damages, but in no case shall the total award of damages in a class action be less than one thousand dollars ($1,000).
>
> (2) An order enjoining the methods, acts, or practices.
>
> (3) Restitution of property.
>
> (4) Punitive damages.

(5) Any other relief that the court deems proper.

2256. California PBI Plaintiffs and the members of the Genworth California Class suffered "damages" and "actual damages" based on the various damages alleged herein.

2257. California PBI Plaintiffs and the members of the Genworth California Class are entitled to the injunctive relief sought herein to enjoin Genworth's unlawful methods, acts, or practices.

2258. California PBI Plaintiffs and the members of the Genworth California Class are entitled to "restitution of property," including, but not limited to, the value of monies they overpaid to Genworth's for its services and the value of the PII they provided to Genworth.

2259. California PBI Plaintiffs and the members of the Genworth California Class are entitled to punitive damages under Cal. Civ. Code § 1780(a)(4). Genworth knew or should have known that Genworth's data security practices were deficient. This is true because, among other things, Genworth was aware that the insurance industry is a frequent target of sophisticated cyberattacks. Genworth knew or should have known that Genworth's data security was insufficient to guard against those attacks. Also, given the size of the database Genworth provided to Genworth's vendor, PBI, and the sensitivity of the PII therein, Genworth should have taken adequate measures to protect the data. Genworth intentionally failed to prevent the decryption of PII or otherwise ensure that it was encrypted while it was in the vendor's possession. Also, Genworth intentionally retained consumers' PII for much longer than was necessary to provide insurance products to customers.

2260. California PBI Plaintiffs and the members of the Genworth California Class are entitled to an award of attorney's fees and costs. Cal. Civ. Code § 1780(e).

2261. Genworth's violations of the CLRA were not the result of a "bona fide error" for purposes of Cal Civ. Code § 1784. Instead, Genworth acted with knowledge, recklessness, gross negligence, negligence, and/or any other form of actionable misconduct.

2262. As a result of Genworth's violations of Cal. Civ. Code § 1770(a)(5) and (7), California PBI Plaintiffs and the members of the Genworth California Class have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages of the various types alleged herein.

2263. California PBI Plaintiffs and the members of the Genworth California Class seek all monetary and non-monetary relief allowed under the CLRA, including injunctive relief enjoining the acts and practices described above.

2264. California PBI Plaintiffs satisfy all requirements for class action treatment set forth in Cal. Civ. Code § 1781(b). As discussed more fully above in the Class Action Allegations section, it is impracticable to bring all members of the Genworth California Class before the Court. The questions of law or fact common to the Class Members are substantially similar for each Class Member, and they predominate over any questions affecting individual Class Members. The claims of the California PBI Plaintiffs are typical of the claims of the Genworth California Class. California PBI Plaintiffs will fairly and adequately represent the interests of the Genworth California Class.

2265. California PBI Plaintiffs have provided timely notice to Genworth of their claims for damages under the CLRA, in compliance with Cal. Civ. Code § 1782(a).

PBI BELLWETHER FIFTEENTH CLAIM FOR RELIEF
California Constitution's Right to Privacy
Cal. Const., Art. I, § I
(Brought by Genworth California Class and PBI California Class)

2266. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2267. California PBI Plaintiffs bring this claim against Genworth Defendants on behalf of the Genworth California Class, and PBI on behalf of the PBI California Class.

2268. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

2269. The right to privacy in California's Constitution creates a private right of action against private and government entities.

2270. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

2271. PBI and Genworth violated PBI Plaintiffs' and California Class Members' constitutional right to privacy by collecting, storing, and disclosing, or preventing from unauthorized disclosure, their personal identifying information and protected health information, which includes in which they had a legally protected privacy interest, and for which they had a reasonable expectation of privacy. Disclosure of their Private Information was highly offensive given the highly sensitive nature of the data. Disclosure of their private medical information in

particular could cause humiliation to Plaintiffs and Class Members. Accordingly, disclosure of Plaintiffs' and Class Members' Private Information is an egregious violation of social norms.

2272. Defendants intruded upon PBI Plaintiffs and California Class Members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential Private Information.

2273. PBI Plaintiffs and California Class Members had a reasonable expectation of privacy in that: (i) their invasion of privacy occurred as a result of Defendants' lax and inadequate security practices with respect to securely collecting, storing, and using data, as well as preventing the unauthorized disclosure of their Private Information; (ii) PBI Plaintiffs and California Class Members did not consent or otherwise authorize Defendants to disclose their Private Information to parties responsible for the cyberattack; and (iii) PBI Plaintiffs and California Class Members could not reasonably expect Defendants would commit acts in violation of laws protecting their privacy.

2274. As a result of Defendants' actions, PBI Plaintiffs and California Class Members have been damaged as a direct and proximate result of Defendants' invasion of their privacy and are entitled to just compensation.

2275. PBI Plaintiffs and California Class Members suffered actual and concrete injury as a result of Defendants' violations of their privacy interests. PBI Plaintiffs and California Class Members are entitled to appropriate relief, including damages to compensate them for the harms to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Defendants' invasions.

PBI Plaintiffs and California Class Members seek appropriate relief for that injury, including, but not limited to, damages that will reasonably compensate them for the harm to their privacy interests as well as disgorgement of profits made by Defendants as a result of their intrusions upon PBI Plaintiffs and California Class Members privacy.

PBI BELLWETHER SIXTEENTH CLAIM FOR RELIEF
Violations of Illinois Personal Information Protection Act ("PIPA"), 815 ILCS 530/10(a)
(Brought on behalf of the PBI Illinois Class and TIAA Illinois Class)

2276. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2277. Plaintiff Uhrich brings this claim against PBI on behalf of the PBI Illinois Class, and TIAA on behalf of the TIAA Illinois Class (the "Illinois Classes").

2278. Section 10(b) of PIPA states, in pertinent part:

> [a]ny data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

815 ILCS 530/10(b).

2279. TIAA conducts substantial business in Illinois. Its business within the state consists of the marketing, sale, delivery, maintenance, and administration of thousands of retirement annuity plans, IRA, wealth management accounts, and other investment accounts, representing billions of dollars in benefits, as well as the maintenance of four offices.[649]

[649] *4 TIAA Offices in IL*, TIAA, https://locations.tiaa.org/il (last visited Dec. 2, 2024).

2280. PBI conducts substantial business in Illinois. It has sought and obtained business from numerous benefit plans conducting business in Illinois.

2281. PBI and TIAA are "data collector[s]" as defined by the statute because each is a company that "handles, collects, disseminates, or otherwise deals with nonpublic personal information." 815 ILCS 530/5.

2282. Plaintiff Uhrich's and the Illinois Classes Members' claims are based on their statuses as "owner[s]" of their PII.

2283. PBI and TIAA failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

2284. Section 45 of PIPA requires entities who maintain or store "personal information concerning an Illinois resident" to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure."

2285. TIAA's and PBI's conduct violated PIPA because they voluntarily undertook the act of maintaining and storing Plaintiff Uhrich's PII, but failed to implement safety and security procedures and practices sufficient enough to protect the PII from the Data Breach that they should have anticipated.

2286. TIAA and PBI should have known and anticipated that data breaches were on the rise and that software companies were lucrative or likely targets of cyber criminals looking to steal PII. Therefore, TIAA and PBI should have implemented and maintained procedures and practices appropriate to the nature and scope of information compromised in the Data Breach.

2287. As a result of TIAA's and PBI's violation of PIPA, Plaintiff Uhrich and the Illinois Classes Members incurred economic damages, including expenses associated with necessary credit monitoring.

PBI BELLWETHER SEVENTEENTH CLAIM FOR RELIEF
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA")
815 ILCS 505/1, *et seq.*
(Brought on behalf of the PBI Illinois Class and TIAA Illinois Class)

2288. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2289. Plaintiff Uhrich brings this claim against PBI on behalf of the PBI Illinois Class, and TIAA on behalf of the TIAA Illinois Class (i.e., the Illinois Classes).

2290. Section 2 of ICFA prohibits unfair or deceptive acts or practices and states, in relevant part, as follows:

> Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of such material fact, or the use or employment of any practice described in section 2 of the "Uniform Deceptive Trade Practices Act", approved August 5, 1965, in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby.

2291. TIAA and PBI violated Section 2 of ICFA by engaging in unfair acts in the course of conduct involving trade or commerce when dealing with Plaintiff Uhrich. Specifically, it was an unfair act and practice for TIAA and PBI to represent to the public that they implemented commercially reasonable measures to protect Plaintiff Uhrich's PII when they knew or should have known that they failed to fulfill such representations, including by preventing and failing to timely detect the Data Breach.

2292. Despite representing to Plaintiff Uhrich and the Illinois Classes Members that they would implement commercially reasonable measures to protect their PII, TIAA and PBI nonetheless failed to fulfill such representations.

2293. Plaintiff Uhrich and the Illinois Classes Members have suffered injury in fact and actual damages, as alleged herein, as a result of TIAA's and PBI's unlawful conduct and violations of the ICFA and analogous state statutes.

2294. TIAA's and PBI's conduct offends public policy as it demonstrates a practice of unfair and deceptive business practices in failing to safeguard consumers' PII.

2295. An award of punitive damages is appropriate because TIAA's and PBI's conduct described above was outrageous, willful and wanton, showed a reckless disregard for the rights of Plaintiff Uhrich and consumers, generally, and Plaintiff Uhrich had no choice but to submit to TIAA's and PBI's illegal conduct.

PBI BELLWETHER EIGHTEENTH CLAIM FOR RELIEF
Violation of the Illinois Uniform Deceptive Trade Practices Act
815 Ill. Comp. Stat. §§ 510/2, *et seq.*
(Brought on behalf of the PBI Illinois Class and TIAA Illinois Class)

2296. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2297. Plaintiff Uhrich brings this claim against PBI on behalf of the PBI Illinois Class, and TIAA on behalf of the TIAA Illinois Class (i.e., Illinois Classes).

2298. TIAA and PBI are each a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

2299. TIAA and PBI engaged in deceptive trade practices in the conduct of their businesses, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including, but not limited to:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

2300. TIAA's and PBI's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Uhrich's PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Uhrich's PII, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Uhrich's PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Uhrich's PII;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Uhrich's PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Uhrich's PII, including duties imposed by the FTCA, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

2301. TIAA's and PBI's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of their data security and ability to protect the confidentiality of consumers' PII.

2302. The above unfair and deceptive practices and acts by TIAA and PBI were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff Uhrich

and the Illinois Classes that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

2303. As a direct and proximate result of TIAA's and PBI's unfair, unlawful, and deceptive trade practices, Plaintiff Uhrich and the Illinois Classes Members have suffered and will continue to suffer injury.

2304. Plaintiff Uhrich and the Illinois Classes Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees and costs.

PBI BELLWETHER NINETEENTH CLAIM FOR RELIEF
Violation of the New Jersey Consumer Fraud Act ("NJCFA")
N.J. Stat. §§ 56:8-1, *et seq.*
(Brought on behalf of the PBI New Jersey Class and TIAA New Jersey Class)

2305. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2306. Plaintiff Phelan brings this claim against PBI on behalf of the PBI New Jersey Class, and TIAA on behalf of the TIAA New Jersey Class (the "New Jersey Classes").

2307. TIAA conducts substantial business in New Jersey. Its business within the state consists of the marketing, sale, delivery, maintenance, and administration of thousands of retirement annuity plans, IRA, wealth management accounts, and other investment accounts, representing billions of dollars in benefits, as well as the maintenance of seven offices.[650]

2308. PBI conducts substantial business in New Jersey. It has sought and obtained business from numerous benefit plans conducting businesses in New Jersey.

2309. The NJCFA states:

[650] *7 TIAA Offices in NJ*, TIAA, https://locations.tiaa.org/nj (last visited Dec. 2, 2024).

> The act, use or employment by any person of any commercial practice that is unconscionable or abusive, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice.

N.J. Stat. § 56:8-2.

2310. Plaintiff Phelan, New Jersey Classes Members, and PBI and TIAA are "persons" under the NJCFA. N.J. Stat. § 56:8-1(d). 233.

2311. The services that PBI and TIAA provided are "merchandise" pursuant to the NJCFA. N.J. Stat. § 56:8-1(c).

2312. PBI and TIAA made uniform representations to Plaintiff Phelan and New Jersey Classes Members that their PII would remain private, as alleged above. They committed deceptive omissions in violation of the NJCFA by failing to inform Plaintiff Phelan and New Jersey Classes Members that they would not adequately secure their PII. Documents that should have contained such disclosures, but did not, include the privacy policies referenced in this complaint and other statements alleged above.

2313. PBI and TIAA separately engaged in unfair acts and practices in violation of the NJCFA by failing to implement and maintain reasonable security measures to protect and secure Plaintiff Phelan's and New Jersey Classes Members' PII in a manner that complied with applicable laws, regulations, and industry standards. The failure to implement and maintain reasonable data security measures offends established public policy, is immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

2314. Due to the Data Breach, Plaintiff Phelan and New Jersey Classes Members have lost property in the form of their PII. Further, PBI's and TIAA's failure to adopt reasonable practices in protecting and safeguarding their PII will force Plaintiff Phelan and New Jersey Classes Members to spend time or money to protect against identity theft.

2315. Plaintiff Phelan and New Jersey Classes Members are now at a substantially higher risk of identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for PBI's and TIAA's practice of collecting and storing PII without appropriate and reasonable safeguards to protect such information.

2316. Plaintiff Phelan and New Jersey Classes Members were damaged by PBI's and TIAA's violation of the NJCFA because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; (vi) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) they overpaid for the services that were received without adequate data security.

PBI BELLWETHER TWENTIETH CLAIM FOR RELIEF
New York Deceptive Trade Practices Act ("GBL")
N.Y. Gen. Bus. Law. § 349
(Brought on behalf of the PBI New York Class and Genworth New York Class)

2317. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2318. Plaintiffs Gilbert Hale and Lynda Hale bring this claim against PBI on behalf of the PBI New York Class, and Genworth Defendants on behalf of the Genworth New York Class (the "New York Classes").

2319. Genworth conducts substantial business in the state of New York. Genworth's business within the state consists of the marketing, sale, delivery, maintenance, and administration of thousands of life insurance policies, representing billions of dollars in benefits, as well as the maintenance of dozens of sales and agent offices.

2320. PBI conducts substantial business in the state of New York. It has sought and obtained business from numerous benefit plans conducting businesses in New York.

2321. PBI and Genworth engaged in deceptive acts or practices in the conduct of their business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs Gilbert and Lynda Hale's and New York Classes Members' PII, which was a direct and proximate cause of the Data Breach, Plaintiffs Gilbert and Lynda Hale's and New York Classes Members' PII being compromised, and subsequent harms caused to Plaintiffs Gilbert and Lynda Hale and New York Classes;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach, Plaintiffs Gilbert and Lynda Hale's and New York Classes Members' PII being compromised, and subsequent harms caused to Plaintiffs Gilbert and Lynda Hale and New York Classes;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Gilbert and Lynda Hale's and New York Classes Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach, Plaintiffs Gilbert and Lynda Hale's and New York Classes Members' PII being compromised, and subsequent harms caused to Plaintiffs Gilbert and Lynda Hale and New York Classes;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs Gilbert and Lynda Hale's and New York Classes Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Gilbert and Lynda Hale's and New York Classes Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that they did not properly secure Plaintiffs Gilbert and Lynda Hale's and New York Classes Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Gilbert and Lynda Hale's and New York Classes Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45.

2322. PBI and Genworth's representations and omissions were material because they were likely to deceive reasonable consumers and clients about the adequacy of their respective data security policies and practices and ability to protect the confidentiality of consumers' PII.

2323. Accordingly, Plaintiffs Gilbert and Lynda Hale and New York Classes Members acted reasonably in relying on PBI and Genworth's misrepresentations and omissions, the truth of which they could not have discovered.

2324. PBI and Genworth acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiffs Gilbert and Lynda Hale's and New York Classes Members' rights.

2325. As a direct and proximate result of PBI and Genworth's unfair, unlawful, and/or fraudulent acts and practices, Plaintiffs Gilbert and Lynda Hale and New York Classes Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including, but not limited to, fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII;

overpayment for Genworth's products and services; loss of the value of access to their PII; value of identity and credit protection and repair services made necessary by the Data Breach; and they face ongoing risks of future harms insofar as they have yet to implement the necessary policies, practices, and measures to adequately safeguard their PII in compliance with laws and industry standards.

2326. PBI and Genworth's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the many New Yorkers affected by the Data Breach.

2327. The above deceptive and unlawful practices and acts by PBI and Genworth caused substantial injury to Plaintiffs Gilbert and Lynda Hale and New York Classes Members that they could not reasonably avoid.

2328. Plaintiffs Gilbert and Lynda Hale and New York Classes Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorneys' fees and costs.

PBI BELLWETHER TWENTY-FIRST CLAIM FOR RELIEF
Violations of the Pennsylvania Unfair Trade Practices and Consumer Protection Law ("UTPCPL"), 73 P.S. §§ 201-1–201-9.3
(Brought on behalf of the PBI Pennsylvania Class and TIAA Pennsylvania Class)

2329. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2330. Plaintiff Checchia brings this claim against PBI on behalf of the PBI Pennsylvania Class, and TIAA on behalf of the TIAA Pennsylvania Class ("Pennsylvania Classes").

2331. TIAA sells and performs services in the Commonwealth of Pennsylvania.

2332. Plaintiff Checchia, Pennsylvania Classes Members, PBI, and TIAA are "persons" as defined by the UTPCPL. 73 P.S. § 201-2(2).

2333. TIAA's products and services constitute as "trade" and "commerce" under the statute. 73 P.S. § 201-2(3).

2334. TIAA and PBI obtained Plaintiff Checchia's and Pennsylvania Classes Members' PII in connection with the services they perform and provide.

2335. TIAA and PBI engaged in unfair or deceptive acts in violation of the UTPCPL by failing to implement and maintain reasonable security measures to protect and secure consumers' (such as Plaintiff Checchia's and Pennsylvania Classes Members') PII in a manner that complied with applicable laws, regulations, and industry standards, including by failing to control all environments into which they placed consumers' PII, and to ensure that those environments were used, configured and monitored in such a way as to ensure the safety of consumers' data.

2336. As alleged above, TIAA and PBI make explicit statements to their customers that their PII will remain private and secure.

2337. The UTPCPL lists twenty-one instances of "unfair methods of competition" and "unfair or deceptive acts or practices." 73 P.S. § 201-2(4). TIAA's and PBI's failure to adequately protect Plaintiff Checchia's and Pennsylvania Classes Members' PII while holding out that they would adequately protect the PII falls under at least the following categories:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation or connection that he does not have (73 P.S. § 201-2(4)(v));

b. Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model, if they are of another (73 P.S. § 201-2(4)(vii));

c. Advertising goods or services with intent not to sell them as advertised (73 P.S. § 201-2(4)(ix)); and

d. Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding (73 P.S. § 201-2(4)(xxi)).

2338. Due to the Data Breach, Plaintiff Checchia and Pennsylvania Classes Members have lost property in the form of their PII. Further, PBI and TIAA's failure to adopt reasonable practices in protecting and safeguarding their customers' PII will force Plaintiff Checchia and Pennsylvania Classes Members to spend time or money to protect against identity theft. Plaintiff Checchia and Pennsylvania Classes Members are now at a higher risk of identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for PBI's and TIAA's practices of collecting and storing PII without appropriate and reasonable safeguards to protect such information.

2339. As a result of PBI and TIAA's violations of the UTPCPL, Plaintiff Checchia and Pennsylvania Classes Members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased or imminent risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost value of the unauthorized access to their PII permitted by TIAA; (vi) the value of long-term credit monitoring and identity theft protection products necessitated by the Data Breach; (vii) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (viii) overpayment for the services that were received without adequate data security.

2340. Pursuant to 73 P.S. § 201-9.2(a), Plaintiff Checchia and Pennsylvania Classes Members seek actual damages, $100, or three times their actual damages, whichever is greatest.

Plaintiff Checchia and Pennsylvania Classes Members also seek costs and reasonable attorney fees.

PBI BELLWETHER TWENTY-SECOND CLAIM FOR RELIEF
Violation of the Vermont Consumer Fraud Act
9 V.S.A §§ 2451, *et seq*.
(Brought on behalf of the PBI Vermont Class and TIAA Vermont Class)

2341. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2342. Plaintiff Marshall brings this claim against PBI on behalf of the PBI Vermont Class, and against TIAA on behalf of the TIAA Vermont Class (the "Vermont Classes").

2343. TIAA conducts substantial business in Vermont. Its business within the state consists of the marketing, sale, delivery, maintenance, and administration of thousands of retirement annuity plans, IRA, wealth management accounts, and other investment accounts, representing millions of dollars in benefits, as well as the maintenance of an office.[651]

2344. PBI conducts substantial business in Vermont. It has sought and obtained business from numerous benefit plans conducting businesses in Vermont.

2345. Plaintiff Marshall and the Vermont Classes Members are "consumers" within the meaning of 9 V.S.A. § 2451a(a) insofar as they agree to pay for products and services from TIAA, and paid—directly or through TIAA—for data security protection they did not receive from PBI and TIAA.

2346. TIAA and PBI are each a "seller" within the meaning of 9 V.S.A. § 2451a(c).

[651] *TIAA Financial Services Williston*, TIAA, https://locations.tiaa.org/vt/williston/166-sycamore-street (last visited Dec. 2, 2024).

2347. The Vermont Consumer Fraud Act ("VCFA") prohibits unfair acts or practices in the conduct of trade or commerce. In interpreting its provisions, the VCFA requires express consideration be given to interpretations by the FTC relating to § 5 of the FTCA. *See* 9 V.S.A. § 2453(b).

2348. TIAA and PBI engaged in unfair business practices prohibited by the VCFA by unreasonably adopting and maintaining data security measures that were inadequate to protect PII and prevent the Data Breach. These unfair practices occurred repeatedly in connection with PBI's and TIAA's trade or business.

2349. TIAA's and PBI's affirmative acts in adopting and maintaining inadequate security measures are unfair within the meaning of the VCFA because they constituted immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers, and provided no benefit to consumers or competition.

2350. TIAA's and PBI's failures also were unfair within the meaning of VCFA because their conduct undermined Vermont public policy that personal and financial information be protected from unauthorized disclosure, as reflected in 9 V.S.A. § 2435.

2351. Plaintiff Marshall and the Vermont Classes reasonably expected TIAA and PBI to maintain secure networks, adhere to industry standards, and otherwise use reasonable care to protect their PII.

2352. TIAA's and PBI's conduct harmed competition. While representing that they had appropriate and sound data security in place, TIAA and PBI cut corners and minimized costs. Meanwhile, their competitors spent the time and money necessary to ensure private information was appropriately secured and safeguarded. Further, the injuries suffered by Plaintiff Marshall and the Vermont Classes are not outweighed by any countervailing benefits to consumers or

competition. And, because TIAA and PBI are solely responsible for securing their networks and protecting PII, there is no way Plaintiff Marshall and the Vermont Classes could have known about PBI and TIAA's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further TIAA's and PBI's legitimate business interests, other than its conduct responsible for the Data Breach.

2353. Plaintiff Marshall and the members of the Vermont Classes are located in Vermont and suffered an injury in Vermont.

2354. TIAA and PBI willfully engaged in the unfair acts and practices described above and knew or should have known that those acts and practices were unfair in violation of the VCFA.

2355. As a direct and proximate result of TIAA's and PBI's unfair practices and violation of the VCFA, Plaintiff Marshall and the Vermont Classes have suffered and will continue to suffer substantial injury and ascertainable loss and are entitled to equitable and such other relief as this Court considers necessary and proper.

PBI BELLWETHER TWENTY-THIRD CLAIM FOR RELIEF
Violations of the Virginia Consumer Protection Act
Va. Code. Ann. §§ 59.1-196, *et seq.*
(Brought on behalf of the Genworth Nationwide Class or, alternatively, the Genworth State Classes)

2356. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2357. PBI Bellwether Plaintiffs Bailey, Camille Burgan, Eugene Burgan, Gilbert Hale, Lynda Hale, Harris, Hauser, Hernandez, and Pasquarelli ("Genworth Plaintiffs") bring this claim against Genworth Defendants on behalf of the Genworth Nationwide Class or, alternatively, the Genworth State Classes (collectively, "Genworth Classes").

2358. The Virginia Consumer Protection Act ("VACPA") is "applied as remedial legation to promote fair and ethical standards of dealings between suppliers and the consumer public." V.S. § 59.1-197. The VACPA prohibits "fraudulent acts or practices committed by a suppliers in connection with a consumer transaction[,]" including: "[m]isrepresenting that goods or services are of a particular standard, quality, grade, style, or model." *Id.* at § 59.1-200(6).

2359. Genworth Defendants engaged in deceptive acts or practices in violation of the VACPA. Specifically, Genworth Defendants performed the following:

a. Implementing and maintaining cybersecurity and privacy measures that were knowingly insufficient to protect Genworth Plaintiffs' and the Genworth Classes' sensitive data, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Genworth Plaintiffs' and the Genworth Classes' sensitive data, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Genworth Plaintiffs' and the Genworth Classes' sensitive data; and

e. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Genworth Plaintiffs' and the Genworth Classes' sensitive data, including duties imposed by the FTCA, 15 U.S.C. § 45. 191. Genworth Defendants are a "supplier" because they are a "seller . . . who advertises, solicits, or engages in consumer transactions . . . ." *Id*. at § 59.1-198.

2360. Genworth Defendants' omissions were material to Genworth Plaintiffs and members of the Genworth Classes because they were likely to and did deceive reasonable consumers about the adequacy of Genworth Defendants' data security and ability to protect the

confidentiality of consumers' sensitive information that Genworth Defendants solicited, collected, and stored.

2361. Had Genworth Defendants disclosed to Genworth Plaintiffs and the Genworth Classes that their cybersecurity, digital platforms, and data storage systems were not secure and, thus, vulnerable to attack, Genworth Defendants would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law.

2362. Instead, Genworth Defendants received, maintained, and compiled Genworth Plaintiffs' and the Genworth Classes' sensitive data as part of the services Genworth Defendants provided and for which Genworth Plaintiffs and members of the Genworth Classes paid, in part, through transaction fees by (1) omitting and concealing information from Genworth Plaintiffs and the Genworth Classes that Genworth Defendants' data security practices were knowingly insufficient to maintain the safety and confidentiality of Genworth Plaintiffs' and the Genworth Classes' sensitive data and (2) that Genworth Defendants were not compliant with basic data security requirements and best practices to prevent a data breach. Accordingly, Genworth Plaintiffs and members of the Genworth Classes acted reasonably in relying on Genworth Defendants' omissions, the truth of which they could not have discovered.

2363. Genworth Plaintiffs and members of the Genworth Classes seek all monetary and nonmonetary relief allowed by law, including statutory damages, actual damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the VCPA.

PBI BELLWETHER TWENTY-FOURTH CLAIM FOR RELIEF
Violations of Virginia's Data Breach Notification Law
Va. Code. Ann. §§ 18.2-186.6, *et seq*.
(Brought on behalf of the Genworth Nationwide Class or, alternatively, the Genworth State Classes)

2364. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2365. Genworth Plaintiffs bring this claim against Genworth Defendants on behalf of the Genworth Nationwide Class or, alternatively, the Genworth State Classes (i.e., Genworth Classes).

2366. The Genworth Defendants are required to accurately notify Genworth Plaintiffs and the Genworth Classes following discovery or notification of a breach of their data security system if decrypted or unredacted PII was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or another fraud, without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

2367. Genworth Defendants are entities that own, license, or maintain computerized data that includes PII as defined by Va. Code Ann. §§ 18.2-186.6(B), (D).

2368. Genworth Plaintiffs' and the Genworth Classes' PII includes PII as covered under Va. Code Ann. § 18.2-186.6(A), including their names in conjunction with their Social Security numbers.

2369. Because Genworth Defendants discovered a breach of their security system in which decrypted or unredacted PII was or is reasonably believed to have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identify theft or another fraud, Genworth Defendants had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Va. Code Ann. §§ 18.2-186.6(B), (D). Yet

Genworth Defendants waited over a month before notifying Genworth Plaintiffs and members of the Genworth Classes of the Data Breach.

2370. By failing to disclose the Data Breach in a timely and accurate manner, Genworth Defendants violated Va. Code Ann. §§ 18.2-186.6(B), (D).

2371. As a direct and proximate result of Genworth Defendants' violations of Va. Code Ann. §§ 18.2- 186.6(B), (D), Genworth Plaintiffs and members of the Genworth Classes suffered damages, as described above.

2372. Genworth Plaintiffs and members of the Genworth Classes seek relief under Va. Code Ann. § 18.2- 186.6(I), including actual damages.

PBI BELLWETHER TWENTY-FIFTH CLAIM FOR RELIEF
Violations of the Washington Consumer Protection Act
Wash. Rev. Code Ann. §§ 19.86.020, *et seq*.
(Brought on behalf of the Milliman Nationwide Class or, alternatively, the Milliman Florida Class)

2373. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2374. Plaintiff Soto brings this claim against Milliman Defendants on behalf of the Milliman Nationwide Class or, alternatively, the Milliman Florida Class (collectively, "Milliman Classes").

2375. Milliman Defendants are "person[s]" as defined by Wash. Rev. Code Ann. § 19.86.010(1).

2376. Milliman Defendants advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2). Milliman Defendants engaged in unfair or

deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Soto's PII and the PII of members of the Milliman Classes, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Soto's PII and the PII of members of the Milliman Classes, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Soto's PII and the PII of members of the Milliman Classes, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Soto's PII and the PII of members of the Milliman Classes, including duties imposed by the FTCA, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Soto's PII and the PII of members of the Milliman Classes; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Soto's PII and the PII of members of the Milliman Classes, including duties imposed by the FTCA, 15 U.S.C. § 45.

2377. Milliman Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Milliman Defendants' data security and ability to protect the confidentiality of consumers' PII.

2378. Milliman Defendants acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded the rights of Plaintiff Soto and members of the Milliman Classes. Milliman Defendants are of such a sophisticated and large

nature that other data breaches and public information regarding security vulnerabilities put them on notice that their security and privacy protections were inadequate.

2379. Milliman Defendants' conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, their conduct affected the public interest, including the many Washingtonians affected by the Data Breach.

2380. As a direct and proximate result of Milliman Defendants' unfair methods of competition and unfair or deceptive acts or practices, Plaintiff Soto and members of the Milliman Classes have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and nonmonetary damages, including loss of the benefit of their bargain with and overcharges by Milliman Defendants, as they would not have paid Milliman Defendants—through MLIC—for services or would have paid less for such services but for the violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

2381. Plaintiff Soto and members of the Milliman Classes seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

PBI BELLWETHER TWENTY-SIXTH CLAIM FOR RELIEF
Violations of the Washington Data Breach Notice Act
Wash. Rev. Code §§ 19.255.010, *et seq*.
(Brought on behalf of the Milliman Nationwide Class or, alternatively, the Milliman Florida Class)

2382. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2383. Plaintiff Soto brings this claim against Milliman Defendants on behalf of the Milliman Nationwide Class or, alternatively, the Milliman Florida Class (i.e., the Milliman Classes).

2384. Milliman Defendants are businesses that own, license, or maintain computerized data that includes PII as defined by Wash. 10 Rev. Code §§ 19.255.010(1), (2).

2385. Plaintiff Soto's PII and the PII of members of the Milliman Classes includes PII as covered under Wash. Rev. Code § 19.255.010(5), including their names in conjunction with their Social Security numbers and dates of birth (among others).

2386. Milliman Defendants are required to accurately notify Plaintiff Soto and members of the Milliman Classes following discovery or notification of the breach of their data security system if PII was, or is reasonably believed to have been, acquired by an unauthorized person and the PII was not secured, in the most expedient time possible and without unreasonable delay under Wash. Rev. Code §§ 19.255.010(2), (11).

2387. Because Milliman Defendants discovered the Data Breach in which PII was, or is reasonably believed to have been, acquired by an unauthorized person and the PII was not secured, Milliman Defendants had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Wash. Rev. Code §§ 19.255.010(2), (11). Yet Milliman Defendants failed to disclose the Data Breach to Plaintiff Soto and members of the Milliman Classes for over a month.

2388. By failing to disclose the Data Breach in a timely and accurate manner, Milliman Defendants violated Wash. Rev. Code §§ 19.255.010(2), (11).

2389. As a direct and proximate result of Milliman Defendants' violations of Wash. Rev. Code §§ 19.255.010(2), (11), Plaintiff Soto and members of the Milliman Classes suffered damages, as described above.

2390. Plaintiff Soto and members of the Milliman Classes seek relief under Wash. Rev. Code §§ 19.255.010(13)(a) and 19.255.010(13)(b), including actual damages and injunctive relief.

PBI BELLWETHER TWENTY-SEVENTH CLAIM FOR RELIEF
Wisconsin Deceptive Trade Practices Act
Wis. Stat. § 100.18, *et seq*.
(Brought on behalf of the MLIC Nationwide Class or, alternatively, the MLIC Florida Class)

2391. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2392. Plaintiff Soto brings this claim against MLIC on behalf of the MLIC Nationwide Class or, alternatively, the MLIC Florida Class (collectively, the "MLIC Classes").

2393. MLIC's conduct violates Wisconsin's Deceptive Trade Practices Act, Wis. Stat. §100.18 (the "WDTPA"), which provides that no,

> firm, corporation or association ... with intent to sell, distribute, increase the consumption of ... any ... merchandise ... directly or indirectly, to the public for sale ... shall make, publish, disseminate, circulate, or place before the public ... in this state, in a ... label ... or in any other way similar or dissimilar to the foregoing, an advertisement, announcement, statement or representation of any kind to the public ... which ... contains any assertion, representation or statement of fact which is untrue, deceptive or misleading.

Plaintiff Soto and members of the MLIC Classes "suffer[ed] pecuniary loss because of a violation" of the WDTPA. Wis. Stat. § 100.18(11)(b)(2).

2394. MLIC deliberately engaged in deceptive and unlawful practices by issuing public announcements, statements, and representations, including on its website, in violation of Wisconsin law by representing to Plaintiff Soto and members of the MLIC Classes and the public that its systems and processes were sufficient to safeguard their PII, when in fact MLIC knew that they were not.

2395. MLIC further violated the WDTPA by: (a) fraudulently advertising material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breach, to prevent infiltration of the security system so as to safeguard PII from unauthorized access; (b) misrepresenting material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard PII in its possession and/or control and data from cyberattacks like the Data Breach, so as to safeguard PII from unauthorized access; (c) omitting, suppressing, and concealing the material fact of the inadequacy of its security practices and procedures; and (d) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain security practices and procedures to safeguard its systems and PII in its possession and/or control from cyberattacks like the Data Breach, to prevent infiltration of the security system so as to safeguard PII from unauthorized access.

2396. The purpose of MLIC's misrepresentations set forth herein was to maximize the number of paying customers that utilized its services—such as Plaintiff Soto and members of the MLIC Classes—and therefore increase its revenues and profits.

2397. MLIC knew or should have known that its security practices and procedures—including that of its vendors—were inadequate and that risk of the Data Breach was high. MLIC's

actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Plaintiff Soto and members of the MLIC Classes.

2398. Plaintiff Soto and members of the MLIC Classes relied upon MLIC's deceptive and unlawful marketing practices and are entitled to damages, including reasonable attorney fees and costs, punitive damages, and other relief which the Court deems proper. Wis. Stat. §§ 100.18(11)(b)(2) and 100.20(5).

PBI BELLWETHER TWENTY-EIGHTH CLAIM FOR RELIEF
Declaratory Relief
28 U.S.C. § 2201
(Brought on behalf of the PBI Bellwether Nationwide Classes or, in the alternative, the PBI Bellwether State Classes)

2399. PBI Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Three.

2400. The PBI Bellwether Plaintiffs bring this claim against each PBI Bellwether Defendant on behalf of the PBI Bellwether Class.

2401. An actual controversy has arisen and exists between the PBI Bellwether Plaintiffs and PBI Bellwether Class Members, on the one hand, and PBI Bellwether Defendants on the other hand, concerning the Data Breach and PBI Bellwether Defendants' failure to protect PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII, including with respect to the issue of whether PBI Bellwether Defendants took adequate measures to protect that information. PBI Bellwether Plaintiffs and the PBI Bellwether Class are entitled to judicial determination as to whether PBI Bellwether Defendants have performed and are adhering to all data privacy

obligations as required by law or otherwise to protect PBI Bellwether Plaintiffs' and PBI Bellwether Class Members' PII from unauthorized access, disclosure, and use.

2402. A judicial determination of the rights and responsibilities of the parties regarding PBI Bellwether Defendants' privacy policies and whether they failed to adequately protect PII is necessary and appropriate to determine with certainty the rights of PBI Bellwether Plaintiffs and the PBI Bellwether Class, and so that there is clarity between the parties as to PBI Bellwether Defendants' data security obligations with respect to PII going forward, in view of the ongoing relationships between the parties.

V. PBI BELLWETHER PRAYER FOR RELIEF

2403. Plaintiffs, individually and on behalf of the PBI Bellwether Class, respectfully request that the Court grant the following relief:

a. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiffs as Class Representative and undersigned counsel as Class Counsel;

b. Find in favor of Plaintiffs and the Classes on all counts asserted herein;

c. Award Plaintiffs and the Classes actual, statutory, and/or punitive monetary damages to the maximum extent as allowed by law;

d. Award Plaintiffs and the Classes compensatory, consequential, general, and/or nominal monetary damages in an amount to be proven at trial;

e. Award Plaintiffs and the Classes restitution and all other applicable forms of equitable monetary relief;

f. Award Plaintiffs and the Classes equitable relief by enjoining PBI from engaging in the wrongful conduct complained of herein regarding the misuse or disclosure of the private information of Plaintiffs and Class Members, and by requiring PBI to issue prompt, complete, and accurate disclosure to Plaintiffs and Class Members;

g. Award Plaintiffs and the Classes injunctive relief as permitted by law or equity to assure that they have an effective remedy, and to protect the interests of Plaintiffs and Class Members, including, but not limited to, an order:

i. requiring PBI to protect from unauthorized disclosure all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws, including by adequate encryption of all such data and by preventing unauthorized access to decryption keys;

ii. requiring PBI to delete, destroy, and purge any personal identifying information of Plaintiffs and Class Members in its possession unless PBI can provide to the Court reasonable justification for the retention and use of such information when weighted against the privacy interests of Plaintiffs and Class Members;

iii. requiring PBI to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on PBI's systems on a periodic basis, and ordering PBI to promptly correct any problems or issues detected by such third-party security auditors;

iv. requiring PBI to engage independent third-party security auditors and internal personnel to run automated security monitoring including, but not limited to, regular database scanning and securing checks;

v. requiring PBI to audit, test, and train its security personnel regarding any new or modified procedures;

vi. requiring PBI to segment data by, among other things, creating firewalls and access controls so that if one area of PBI network is compromised, hackers cannot gain access to other portions of PBI's systems;

vii. requiring PBI to establish for all PBI employees an information security training program that includes annual training, with additional training to be provided as appropriate;

viii. requiring PBI to establish for all PBI security personnel a security training program that includes regularly scheduled internal training and education to inform PBI's internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

ix. requiring PBI to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with PBI's policies, programs, and systems for protecting personal identifying information;

x. requiring PBI to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor PBI's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xi. requiring PBI to provide notice to Plaintiffs and all Class Members regarding the full nature and extent of the Data Breach and the disclosure of Private Information to unauthorized persons, including the threat posed as a result of the disclosure of their confidential personal information, and educating Plaintiffs and Class Members regarding steps affected individuals should take to protect themselves;

xii. requiring PBI to implement logging and monitoring programs sufficient to track traffic to and from PBI's servers;

xiii. requiring, for a period of 10 years, the appointment of a qualified and independent third-party assessor to conduct an annual SOC 2 Type 2 attestation to evaluate PBI's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Classes, and to report any deficiencies with compliance of the Court's final judgment;

xiv. requiring PBI to implement multi-factor authentication requirements, if not already implemented; and

xv. requiring PBI employees to employ passwords consistent with best security practices and to change their passwords on a timely and regular basis..

h. Award disgorgement and restitution of all earnings, profits, compensation, and benefits received by PBI as a result of its unlawful acts;

i. Order PBI to purchase or provide funds for lifetime credit monitoring and identify theft insurance to Plaintiffs and Class Members;

j. Order PBI to pay all costs necessary to notice Class Members about the judgment and all costs necessary to administer a court approved claims process.

k. Award Plaintiffs and the Classes pre-judgment and post-judgment interest to the maximum extent allowed by law;

l. Grant Plaintiffs and the Classes leave to amend this complaint to conform to the evidence produced during the course of this case;

m. Award Plaintiffs and the Classes reasonable attorneys' fees, costs, and expenses, as allowable;

n. Where necessary, distribute any monies recovered from PBI on behalf of Class Members or the general public via fluid recovery or cy pres recovery as applicable to prevent PBI from retaining benefits of its wrongful conduct;

o. Award Plaintiffs and the Class such other favorable relief as allowable under law or at equity;

p. Award any other and further relief as may be just and proper; and

q. Conduct a trial by jury on all issues so triable.

CHAPTER FOUR:

FACTUAL ALLEGATIONS AND CAUSES OF ACTION AGAINST DELTA ENTITIES

I. Delta Dental Bellwether Defendants' Businesses Require the Collection and Maintenance of Delta Dental Bellwether Plaintiffs' and Class Members' Private Information

2404. Delta Dental of California, together with its affiliate companies,[652] touts itself as the "nation's largest, most experienced dental benefits carrier," that offers individual and group dental insurance plans, providing dental insurance to tens of million individuals.[653] "Collectively, [Delta Dental of California and its affiliate companies] offer benefits to more Americans than any other dental insurance company."[654]

2405. Delta Dental of California (i.e., DDCA) offers and administers Delta Dental Preferred Provider Organization ("PPO") and other fee-for-service dental programs to groups headquartered or located in California.

2406. Delta Dental Insurance Company (i.e., DDIC) is an affiliate of Delta Dental of California. DDIC offers and administers Delta Dental PPO and other fee-for-service dental programs to groups headquartered or located in Alabama, Florida, Georgia, Louisiana, Mississippi,

---

[652] "The Delta Dental of California enterprise includes its affiliates Delta Dental Insurance Company; Delta Dental of the District of Columbia, Delta Dental of Delaware, Inc., Delta Dental of Pennsylvania, Delta Dental of New York, Inc., Delta Dental of West Virginia, and their affiliated companies, as well as the national DeltaCare USA network." *See* Data Breach Notifications, Office of the Maine Attorney General; Copy of notice to affected Maine residents: "AG Notice – ME – Delta Dental + Affiliates," PDF available for download here: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/4d61e15b-a303-4653-8206-9d54aa0d1e26.shtml (last visited Dec. 4, 2024).

[653] Delta Dental, *Forbes names Delta Dental of California one of America's best employers for 2024*; available here: https://perma.cc/W434-ZPCK (last visited Jun. 4, 2024).

[654] Delta Dental, *Corporate Profile*; available here: https://perma.cc/63Q4-38XM (last visited Jun. 4, 2024).

Montana, Nevada, and Utah, and vision programs to groups headquartered in West Virginia. In Texas, Delta Dental Insurance Company offers and administers fee-for-service dental programs and provides a dental provider organization ("DPO") plan.

2407. Delta Dental of New York (i.e., DDNY) is an affiliate of Delta Dental of California. DDNY offers and administers Delta Dental PPO and other fee-for-service programs in New York.

2408. Delta Dental of Pennsylvania (i.e., DDPenn) is an affiliate of Delta Dental of California. DDPenn and its own affiliates offer and administer Delta Dental PPO and other fee for-service dental programs in Delaware (Delta Dental of Delaware), Maryland, Pennsylvania, West Virginia (Delta Dental of West Virginia) and the District of Columbia (Delta Dental of the District of Columbia).

2409. "The companies in [Delta Dental's] enterprise are members, or affiliates of members, of the Delta Dental Plans Association, a network of 39 Delta Dental companies that together provide dental coverage to 80 million people around the country."[655]

2410. Delta Dental Plans Association (i.e., DDA) was created in order to coordinate dental insurance for companies with employees in multiple states. Accordingly, customers may receive dental insurance from a Delta Dental Company distinct from the one that offers and administers the Delta Dental insurance plan in their state. For example, a resident of New York may in fact receive health insurance through DDPenn, rather than through DDNY.

2411. DDA allows customers to see a provider in any state regardless of the member company through which they receive dental insurance.

[655] Delta Dental, *2019 Social Impact Report*; available here: https://perma.cc/TNZ2-CMAX (last visited Jun. 4, 2024).

2412. DDA's website, © Copyright 2024 Delta Dental Plans Association, represents the network of 39 Delta Dental Companies and is branded as "Delta Dental."

2413. The other related website, © Copyright 2024 Delta Dental, "is the home of" the Delta Dental of California and affiliates, collectively. This website also brands itself as "Delta Dental." Each of these Defendants is a member of DDA's network of 39 Delta Dental insurance companies.

2414. As described on both DDA's website and the website for Delta Dental of California and affiliates, "Through our national network of Delta Dental companies, we offer dental coverage across all 50 states, Puerto Rico and other U.S. territories . . . offering dental insurance across all 50 states, D.C., and Puerto Rico."[656]

2415. DDA holds itself out as having interconnected business operations with DDCA and Affiliates—the other Delta Dental Bellwether Defendants.

2416. DDA refers to itself as one and the same as the other Delta Dental Bellwether Defendants with respect to its value of data security and prioritizing practices to protect customers' data, *i.e.*, that its security policies and practices are consistent through its network of Delta Dental Companies, including the other Delta Dental Bellwether Defendants.

2417. Specifically, "Because security is important to both Delta Dental and you, we employ reasonable safeguards designed to promote the security of our systems and protect your personal information from unauthorized destruction, use, modification, or disclosure. Personal

[656] Delta Dental, *About Delta Dental*; available here: https://perma.cc/4R33-GGCQ (last visited Jun. 4, 2024).

information is protected using various physical, administrative and/or technical safeguards in transit and at rest."[657]

2418. Upon information and belief, all the Delta Dental Companies within DDA's network, including DDCA and Affiliates, utilize the MOVEit software and follow the same safety and security policies, practices, and procedures.

2419. Customers, *i.e.*, policy holders through a Delta Dental Company, can sign up for an Account with Delta Dental Plans Association on DDA's website, for example, to access a Member Dashboard. To complete account registration, DDA requires policy holders to provide PHI, including the following information: first name, last name, Member ID and health insurance information, Social Security number, date of birth, ZIP code, and email address.[658]

2420. Through their DDA accounts, members may "request information about [their] coverage or claims through the Services (which request will go to the Delta Dental Company that administers or underwrites [their] dental benefits coverage)," and DDA requires that they provide certain sensitive personal and medical related information as part of the request. [659] Additionally, members use DDA's platform to track their dental activity, *i.e.*, protected health information as defined under HIPAA.[660]

---

[657] Delta Dental; *Privacy Statement for the Delta Dental Plans Association Website and Mobile App – Consumers*; available here: https://perma.cc/A2HD-6PW3 (last visited Jun. 4, 2024).

[658] *Id.*

[659] *Id.*

[660] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq*., and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 42 U.S.C. § 1320d(6); 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and

2421. Customers can use DDA's landing page to locate more information about their Delta Dental insurance provider and download the Delta Dental mobile application, through which their Private Information flows. In other words, customers, including Delta Dental Bellwether Plaintiffs and Class Members, interact directly with DDA and provide their Private Information to DDA, in addition to the Delta Dental Company, including DDCA and Affiliates, that provides their insurance plan.

2422. Additionally, DDA's diversity, equity, and inclusion "guiding principles" apply to all 39 member companies, including DDCA and Affiliates, according to DDA's website.

2423. As part of their business operations, DDCA and Affiliates acquire, collect, store, and utilize consumers' sensitive personal data, including PII and PHI. As a condition of receiving dental insurance through DDCA and Affiliates, Delta Dental Bellwether Plaintiffs and Class Members were required to provide, directly or indirectly, and entrust their highly sensitive Private Information with DDCA and Affiliates. DDCA and Affiliates relied on and derived monetary benefits and profit from Delta Dental Bellwether Plaintiffs' and Class Members' providing their Private Information.

2424. DDA also collects, transmits, and uses this data as part of its business operations, and informs users in its Privacy Policy that it "shar[es] collected personal information with third parties, including service providers, business associates, and the Delta Dental Companies."[661] DDA entered into a "Business Associate Agreement" with each of the Delta Dental Companies, including DDCA and Affiliates. A Business Associate Agreement identifies that both entities are

---

demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. DEP'T FOR HEALTH & HUM. SERVS., "Summary of the HIPAA Privacy Rule;" available here: https://perma.cc/9U8X-5L7E (last visited June 4, 2024).

[661] Delta Dental; *Privacy Statement for the Delta Dental Plans Association Website and Mobile App – Consumers*; available here: https://perma.cc/A2HD-6PW3 (last visited June 4, 2024).

regulated under the U.S. Health Insurance Portability and Accountability Act (HIPAA), wherein both parties must agree that they "understand the privacy and security safeguards established by HIPAA, HITECH, and the Omnibus Rule and agree to protect member Personal Health Information (PHI)"[662] and set out the terms in which Delta Dental Bellwether Plaintiffs' and Class Members' Private Information can be transferred and disclosed.[663] In other words, the other DDCA and Affiliates and DDA share data. Similarly, DDA derives financial benefit from Delta Dental Bellwether Plaintiffs' and Class Members' providing their Private Information to the Delta Dental Companies with which it contracts, including DDCA and Affiliates.

2425. DDCA and Affiliates contract with the third-party service provider, Progress, to utilize its MOVEit software to store and transfer the Private Information of Delta Dental Bellwether Plaintiffs and Class Members.

2426. Similar to DDA, Progress also entered into Business Associate Agreements (hereafter "BAA") with DDCA and Affiliates, which set out the terms in which Delta Dental Bellwether Plaintiffs' and Class Members' Private Information can be transferred and disclosed.[664]

---

[662] *Id.*; *see also* Delta Dental, *Legal*; available here: https://perma.cc/8TUV-ED9Y (last visited June 4, 2024).

[663] *See* Delta Dental; *Privacy Statement for the Delta Dental Plans Association Website and Mobile App – Consumers*; available here: https://perma.cc/A2HD-6PW3 (last visited Jun. 4, 2024) ("Applicable HIPAA business associate agreements generally permit Delta Dental to use and disclose your individually identifiable health information (1) to perform functions or activities on behalf of, or provide services to, the Delta Dental Companies, in connection with their role in underwriting dental benefit coverage and administering dental benefit programs and claims, or as otherwise permitted or required by law including HIPAA; (2) for Delta Dental's proper management and administration or to fulfill its legal responsibilities; (3) to perform data aggregation services in order to provide analysis relevant to the health care operations of the Delta Dental Companies . . . ."); *see also* 45 C.F.R. 164.504(e) (requirements for contract).

[664] *See* Progress, *HIPAA Compliance FAQS*; available here: https://perma.cc/PAG9-PYHZ (last visited June 4, 2024).

2427. As business associates of healthcare providers, both DDA and Progress knowingly obtain sensitive patient Private Information and have a resulting duty to securely maintain such information in confidence.

2428. This Private Information was compromised as a result of a security vulnerability in the MOVEit software, as alleged in Chapter One and incorporated and realleged herein.

2429. The MOVEit Transfer servers that were targeted in the Data Breach were located within the Delta Dental of California network environment. As discussed, infra, these servers contained the Private Information of DDCA and Affiliates' customers, including that of Delta Dental Bellwether Plaintiffs and Delta Dental of California and Affiliates Nationwide Class Members.

2430. Although thousands of companies were affected by the Data Breach, Delta Dental "stands out [because it] is the third largest healthcare MOVEit-related breach to have been reported" – affecting 6,928,932 customers.[665]

2431. The Private Information compromised in the Data Breach included "names with some combination of the following: addresses, Social Security numbers, driver's license numbers or other state identification numbers, passport numbers, financial account information, tax identification numbers, individual health insurance policy numbers, and/or health information."[666]

[665] "Delta Dental of California Data Breach: 7 Million Individuals Affected." THE HIPAA JOURNAL, published Dec. 17, 2023; available here: https://perma.cc/WZE9-R483 (last visited Jun. 4, 2024).

[666] Data Breach Notifications, Office of the Maine Attorney General; Copy of notice to affected Maine residents: "AG Notice – ME – Delta Dental + Affiliates," PDF available for download: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/4d61e15b-a303-4653-8206-9d54aa0d1e26.shtml (last visited Dec. 4, 2024).

2432. Some or all of the healthcare and/or medical information that was compromised and stolen by the unauthorized actors constitutes "protected health information" within the meaning of HIPAA.[667]

A. Delta Dental Bellwether Defendants Misrepresented Their Security Practices

2433. Delta Dental Bellwether Defendants made numerous representations and promises that customers' Private Information was "private and confidential[,]" and about their commitment to maintaining its safety, including on their various webpages.[668]

2434. For examples, DDA's "Compliance Center" discusses "Delta Dental's compliance" with the various mandates under HIPAA.[669] Under its Privacy Policy, DDA states that it "collects, uses, and discloses your individually identifiable health information consistent with the terms of applicable HIPAA business associate agreements with the Delta Dental Companies."[670]

2435. DDA also states in one of its privacy statements that, "Because security is important to both Delta Dental and you, we employ reasonable safeguards designed to promote the security

[667] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq*., and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 42 U.S.C. § 1320d(6); 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. DEP'T FOR HEALTH & HUM. SERVS., "Summary of the HIPAA Privacy Rule;" available here: https://perma.cc/9U8X-5L7E (last visited Jun. 4, 2024).

[668] Delta Dental, *Corporate Profile*; available here: https://perma.cc/63Q4-38XM (last visited Jun. 4, 2024).

[669] *See* Delta Dental, *Compliance Center*; available here: https://perma.cc/Q3JG-ZK6Z (last visited Jun. 4, 2024).

[670] Delta Dental; *Privacy Statement for the Delta Dental Plans Association Website and Mobile App – Consumers*; available here: https://perma.cc/A2HD-6PW3 (last visited June 4, 2024).

of our systems and protect your personal information from unauthorized destruction, use, modification, or disclosure. Personal information is protected using various physical, administrative and/or technical safeguards in transit and at rest."[671]

2436. DDCA and Affiliates' website assures existing and prospective customers that it "has updated and implemented system changes to accommodate the applicable 5010 standards and the associated transaction sets" and that HIPAA covered transactions include enrollment information in health plans and health care claims, which include costs of treatments – precisely the type of data that was compromised in the Data Breach.[672]

B. Delta Dental Bellwether Defendants Owed Legal Obligations to Delta Dental Bellwether Plaintiffs and Class Members

2437. DDA's national network of 39 Delta Dental Companies (including DDCA and Affiliates) provides dental insurance to 80 million individuals. Delta Dental Bellwether Plaintiffs and Class Members are currently or were formerly customers of DDCA and Affiliates.

2438. As a condition of using DDCA and Affiliates' services, *i.e.*, entering into a direct business relationship with a Delta Dental member company, Delta Dental Bellwether Plaintiffs and Class Members were required to provide their highly sensitive Private Information.

2439. Because DDCA and Affiliates required Delta Dental Bellwether Plaintiffs' and Class Members' Private Information in exchange for the provision of dental insurance, by accepting their Private Information, DDCA and Affiliates owed and otherwise assumed statutory, regulatory, contractual, and common law duties and obligations, and knew or should have known that they were responsible for protecting Delta Dental Bellwether Plaintiffs' and Class Members'

---

[671] *Id.*

[672] Delta Dental; *Compliance Center*, "HIPAA Compliance Update: Electronic Transaction Standard;" available here: https://perma.cc/U37F-DBBK (last visited June 4, 2024).

Private Information and keeping it confidential, safe, and secure from the type of unauthorized access, disclosure, and theft that occurred in the Data Breach, including by ensuring that their third-party service providers implemented adequate, secure, and compliant safeguards to protect their own platforms.

2440. Because of the highly sensitive and personal nature of the information that Delta Dental Bellwether Defendants acquire, maintain on their shared network, and input into Progress's MOVEit file transfer server and/or software, Delta Dental Bellwether Defendants have a non-delegable duty to Delta Dental Bellwether Plaintiffs and Class Members to implement reasonable and adequate security measures to protect their Private Information, including to ensure their third-party vendors had implemented adequately safe and secure policies and practices. DDCA and Affiliates' promise, among other things, to: keep customers' files private; comply with regulation and industry standards, including FTC guidelines, related to data security and maintenance of their customers' files and the Private Information contained therein; inform consumers of their legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to the products and services Delta Dental Bellwether Plaintiffs and Class Members obtain from Defendants; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

2441. Similarly, DDA owed duties analogous to DDCA and Affiliates by representing itself to customers as one and the same, such that a reasonable person would rely on these representations in understanding the nature of their relationship. DDA also benefitted monetarily from its collection, storage, receipt, transfer, and use of Delta Dental Bellwether Plaintiffs' and Class Members' Private Information as laid out in its BAAs.

2442. As sophisticated business entities handling highly sensitive and confidential consumer data, Delta Dental Bellwether Defendants' data security obligations were particularly important, especially in light of the substantial increase in cyberattacks and data breaches in industries handling significant amounts of Private Information preceding the date of the MOVEit Data Breach.

2443. In light of recent high profile data breaches—including breaches arising from previously exploited vulnerabilities in other file transfer applications (*e.g.*, Accellion FTA, Fortra GoAnywhere MFT)— at all relevant times, Delta Dental Bellwether Defendants knew or should have known that Delta Dental customers', including Delta Dental Bellwether Plaintiffs, and Class Members', Private Information would be targeted by cybercriminals and ransomware attack groups.

2444. Despite such knowledge, Delta Dental Bellwether Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Delta Dental Bellwether Plaintiffs' and Class Members' Private Information from cyberattacks, including, but not limited to, adequately vetting, auditing, monitoring, testing, and patching the software applications they used to store and transfer such data.

2445. "Third-party software security risks are on the rise, and so are the significant cyber attacks they facilitate. According to a CrowdStrike report, 45% of surveyed organizations said they experienced at least on software supply chain attack in 2021."[673]

2446. Recent high profile cybersecurity incidents at healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019),

[673] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard (last updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software (last visited Dec. 2, 2024).

University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), put Healthcare Defendants on notice that their electronic records would be targeted by cybercriminals.

2447. According to the HIPAA Journal's 2023 Healthcare Data Breach Report, "[a]n unwanted record was set in 2023 with 725 large security breaches in healthcare reported to the Department of Health and Human Services Office for Civil Rights, beating the record of 720 healthcare security breaches set the previous year."[674]

2448. Cyberattacks and data breaches of financial services companies or companies storing financial data are also especially problematic because of the potentially permanent disruption they cause to the daily lives of their customers. Stories of identity theft and fraud abound, with hundreds of millions of dollars lost by everyday consumers every year as a result of internet-based identity theft attacks.[675]

2449. The Government Accountability Office ("GAO") found that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[676]

---

[674] Steve Adler, *Security Breaches in Healthcare in 2023*, THE HIPAA JOURNAL (January 31, 2024), https://www.hipaajournal.com/wp-content/uploads/2024/01/Security_Breaches_In_Healthcare_in_2023_by_The_HIPAA_Journal.pdf (last visited Dec. 2, 2024).

[675] Albert Khoury, *Scam alert: 5 most costly data breaches (plus 5 states most targeted)* (July 27, 2022), https://www.komando.com/security-privacy/most-costly-data-breaches/847800/.

[676] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* ("GAO Report") at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf [https://perma.cc/GCA5-WYA5].

2450. As highly sophisticated parties that handle sensitive Private Information, Delta Dental Bellwether Defendants failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Delta Dental Bellwether Plaintiffs' and Class Members' Private Information.

2451. The ramifications of Delta Dental Bellwether Defendants' failures to keep Delta Dental Bellwether Plaintiffs' and Class Members' Private Information secure are severe and long-lasting. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in part because the data can be sold in small batches to multiple buyers as opposed to in bulk to a single buyer. Thus, Delta Dental Bellwether Plaintiffs and Class Members must vigilantly monitor their financial accounts, and Delta Dental Bellwether Plaintiffs and Class Members are at an increased risk of fraud and identity theft, for many years into the future.

2452. Thus, Delta Dental Bellwether Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to them and of the foreseeable consequences if their systems were breached. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring or from mitigating the consequences of the Data Breach.

2453. As alleged and incorporated, Progress owed a non-delegable duty to Delta Dental Bellwether Plaintiffs and Class Members to identify and remediate vulnerabilities in its MOVEit software and to implement reasonable and adequate security measures to secure and protect Delta Dental Bellwether Plaintiffs' and Class Members' Private Information. *See* Chapter One and Chapter Two (describing Progress's legal and equitable duties of which it knew or should have known).

2454. Progress's obligations also arise because it is regulated under the terms of a "Business Associate" under HIPAA.[677] 45 C.F.R. § 160.103(1).

2455. As incorporated and realleged herein, Delta Dental Bellwether Defendants knew of these requirements and of industry cybersecurity standards and their obligations to protect Delta Dental Bellwether Plaintiffs' and Class Members' highly sensitive Private Information. *See* Chapter One. Delta Dental Bellwether Defendants were also aware of the significant repercussions that would result from their failure to do so.

2456. Delta Dental Bellwether Plaintiffs and Class Members relied on Delta Dental Bellwether Defendants to implement and maintain adequate data security policies and protocols (including vetting, auditing, and monitoring vendors and software companies on which they relied) to keep their Private Information confidential and securely maintained, to use such Private Information (if at all) solely for business and healthcare purposes, and to prevent unauthorized access and disclosure of Private Information to unauthorized persons. Delta Dental Bellwether Plaintiffs and Class Members reasonably expected Delta Dental Defendants would safeguard their highly sensitive information and keep that Private Information confidential.

2457. In addition to the aforementioned and incorporated industry standards, the Center for Internet Security (CIS) has also published clear guidance on the steps businesses that share

[677] Under HIPAA, a "business associate" is defined as, with respect to a covered entity, a person who: "creates, receives, maintains, or transmits protected health information for a function or activity regulated by [HIPAA], including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 C.F.R. 3.20, billing, benefit management, practice management and repricing. . . . ." 45 C.F.R. § 160.103(1). *Business Associate*. A business associate includes an entity "that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information." 45 C.F.R. § 160.103(3). As a software that transfers HIPAA protected data contracted with HIPAA covered entities, Progress is clearly a "business associate," subject to HIPAA, with respect to its relationship and data acquired and stored through its contract with DDCA and Affiliates.

information with third parties, *e.g.*, "rely on vendors and partners to help manage their data or rely on third-party infrastructure for core applications or functions," should take to ensure those vendors have appropriate cybersecurity systems and protocols in place, and that their customers' Private Information is adequately safeguarded. Since its formation in 2000, CIS has established applicable industry standards to help people, businesses, and governments protect themselves against pervasive cyber threats that are "globally recognized best practices for security IT systems and data."[678]

2458. Delta Dental Bellwether Defendants also knew, or should have known, the importance of safeguarding the Private Information entrusted to them, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on affected individuals as a result of a data breach.

2459. Each Delta Dental Bellwether Defendant therefore owed a duty to Delta Dental Bellwether Plaintiffs and Class Members to implement and maintain reasonable and adequate data security measures to secure, protect, and safeguard the Private Information entrusted to them by Delta Dental Bellwether Plaintiffs and Class Members.

2460. Delta Dental Bellwether Defendants should have used their resources to implement and maintain adequate data security procedures and practices.

2461. Delta Dental Bellwether Defendants should have but did not vet Progress or its MOVEit Transfer software, and as a result, failed to prevent or detect the Data Breach.

[678] Center for Internet Security, *Critical Security Controls*, at pp. 12, 42-44 (May 2021); available here: https://perma.cc/R3M4-4KAU (last visited June 4, 2024).

2462. Delta Dental Bellwether Defendants knew or should have known that Progress: employed poorly-written, outdated, and insecure code in its MOVEit software; failed to update outdated code; and failed to check for known or newly discovered vulnerabilities.

2463. Delta Dental Bellwether Defendants failed to ensure Progress employed and maintained adequate cybersecurity measures to prevent the Data Breach from occurring.

2464. Delta Dental Bellwether Defendants breached their duties to Delta Dental Bellwether Plaintiffs and Class Members by, among other things, failing to employ adequate screening and vetting practices of its vendors or vendors of its Business Associates, including Progress and its MOVEit Transfer software.

Delta Dental Bellwether Defendants also had obligations arising under the FTC Act, HIPAA, industry standards, common law, and their own promises and representations made to Delta Dental Bellwether Plaintiffs and Class Members to keep their Private Information confidential and protected from unauthorized access and disclosure.

C. Delta Dental Bellwether Defendants Failed to Comply with FTC Guidelines

2465. As previously alleged and incorporated, Progress's customers, including DDCA and Affiliates, were required to comply with the FTC guidelines. *Inter alia*, the FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[679] *See* Chapter One and Chapter Two.

2466. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

[679] *Start With Security*, Fed. Trade Comm'n ("FTC"); available here: https://perma.cc/W829-XP9N (last visited June 4, 2024).

2467. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[680]

2468. The FTC guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach.[681]

2469. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

2470. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15

---

[680] FTC, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[681] *Id.*

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

2471. DDCA and Affiliates failed to properly implement the foregoing recommended data security practices.

2472. Delta Dental Bellwether Defendants were at all times fully aware of their obligations to protect the Private Information entrusted to them. They were also aware of the significant repercussions that would result from their failure to do so.

D. Delta Dental Bellwether Defendants Violated Their HIPAA Obligations

2473. Moreover, DDCA and Affiliates owed legal obligations to Delta Dental Bellwether Plaintiffs and Class Members as "covered entities" under the Health Insurance Portability and Accountability Act ("HIPAA") and subject to its regulations.[682]

2474. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

2475. As previously alleged, DDA also entered into BAAs with each of the Delta Dental Companies of its national network which governed the transfer, use, and disclosure of Delta Dental Bellwether Plaintiffs' and Class Members' PHI.[683] DDA is governed by HIPAA's regulations of business associates.

[682] A "covered entity" is defined as, *inter alia*, "[a] health care provider who transmits any health information in electronic form in connection with a transaction covered by [HIPAA]." 45 C.F.R. § 160.102(a)(3). "Health Plans, including health insurance companies" are covered entities under HIPAA. *Your Rights Under HIPAA*, DEP'T FOR HEALTH & HUM. SERVS., https://perma.cc/ER6M-X3KL (last visited June 4, 2024). As a provider of dental insurance, DDCA and Affiliates are clearly "covered entit[ies]," subject to HIPAA.

[683] Delta Dental; *Privacy Statement for the Delta Dental Plans Association Website and Mobile App – Consumers*; available here: https://perma.cc/A2HD-6PW3 (last visited June 4, 2024).

2476. As business associates, DDA and Progress are also required to follow regulations for safeguarding electronic medical information pursuant to the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH"). *See* HITECH Act, Sec. 13400, *et seq*.; 42 U.S. Code § 17931; 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

2477. Both HIPAA and HITECH obligate DDA to follow reasonable security standards, respond to, contain, and mitigate security violations, and to protect against disclosure of sensitive patient Private Information. These standards and rules require of business associates comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of Private Information is properly maintained and protected. 42 U.S. Code § 17931 (applying security requirements to business associates and incorporating security requirements into BAAs between business associates and covered entities); *see* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards); 45 C.F.R. § 164.316 (policies and procedures and documentation requirements).

2478. As "business associates" under HIPAA, "the standards, requirements, and implementation specifications adopted under [HIPAA] apply" to both Progress and DDA. 45 C.F.R. § 160.102(b). For example, "[a] written contract between a covered entity and business associate must . . . [among numerous other requirements] require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information . . . ." [684] *See* the HIPAA Security Rule, 45 C.F.R. Part 160 and Part

[684] Under HIPAA, a "business associate" is defined as, with respect to a covered entity, a person who: "creates, receives, maintains, or transmits protected health information for a function or activity regulated by [HIPAA], including claims processing or administration, data analysis,

164, Subparts A and C ("Security Standards for the Protection of Electronic Protected Health Information"). Business Associates are also required to comply with the Health Information Technology Economic and Clinical Health Act ("HITECH").[685] In other words, DDA's non-delegable duties also arise under HIPAA and the HITECH Act.

2479. Further, the U.S. Department of Health and Human Services recommends the following data security measures that business associates, such as DDA, should implement to protect against some of the more common, and often successful, cyber-attack techniques. According to those guidelines, business associates should:

a. implement security awareness and training for all workforce members and that the training programs should be ongoing, and evolving to be flexible to educate the workforce on new and current cybersecurity threats and how to respond;

b. implement technologies that examine and verify that received emails do not originate from known malicious sites, scan web links or attachments included in emails for potential threats, and impede or deny the introduction of malware that may attempt to access PHI;

c. mitigate known data security vulnerabilities by patching or upgrading vulnerable technology infrastructure, by upgrading or replacing obsolete and/or unsupported applications and devices, or by implementing

---

processing or administration, utilization review, quality assurance, patient safety activities listed at 42 C.F.R. 3.20, billing, benefit management, practice management and repricing. . . . ." 45 C.F.R. § 160.103(1). *Business Associate*. A business associate includes an entity "that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information." 45 C.F.R. § 160.103(3). As a software that transfers HIPAA protected data contracted with a HIPAA covered entity, Progress is clearly a "business associate," subject to HIPAA, with respect to its relationship and data acquired and stored through its contracts with DDCA and Affiliates; *see also* 45 C.F.R. § 160.102(a)(3). A "covered entity" is defined as, *inter alia*, "[a] health care provider who transmits any health information in electronic form in connection with a transaction covered by [HIPAA]." "Health Plans, including health insurance companies" are covered entities under HIPAA. *Your Rights Under HIPAA*, DEP'T FOR HEALTH & HUM. SERVS., https://perma.cc/ER6M-X3KL (last visited June 4, 2024). As providers of dental insurance, DDCA and Affiliates are clearly "covered entit[ies]," subject to HIPAA.

[685] *See* 42 U.S.C. § 17921(2) (incorporating "business associate" as defined in 45 C.F.R. § 160.103).

safeguards to mitigate known vulnerabilities until an upgrade or replacement can occur;

d. implement security management processes to prevent, detect, contain, and correct security violations, including conducting risk assessments to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI; and

e. implement strong cyber security practices by requiring strong passwords rules and multifactor identification.[686]

2480. As "covered entities" under HIPAA, respectively, DDCA and Affiliates are required to comply with both the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C ("Security Standards for the Protection of Electronic Protected Health Information"), as well as the HITECH Act, as alleged in Plaintiffs' Omnibus Set of Additional Pleading Facts and incorporated as if fully set forth herein. *See* Chapter One and Chapter Two.[687]

2481. As "covered entities" under HIPAA, DDCA and Affiliates were additionally legally obligated to comply with the Breach Notification Rule, 45 C.F.R. Part 164, Subpart D ("Notification in the Case of Breach of Unsecured Protected Health Information"), which required them to provide notice of the breach to affected individuals "without unreasonable delay and in no case later than 60 days following discovery of the breach."[688] Additionally, covered entities are required to "mitigate . . . any harmful effect . . . . of a use or disclosure of protected health

[686] OCR Quarter 1 2022 Cybersecurity Newsletter, U.S. DEP'T HEALTH HUM.SERVS., (Mar. 17, 2022), https://perma.cc/5L25-V4Z4 (last visited June 4, 2024).

[687] *See also* "Summary of the HIPAA Security Rule," DEP'T FOR HEALTH & HUM. SERVS., https://perma.cc/J2XB-5TLA (last visited June 4, 2024).

[688] 45 C.F.R. § 164.404 Notification to individuals. *Breach Notification Rule*, https://perma.cc/KM4C-F3FR (last visited June 4, 2024). "With respect to a breach at or by a business associate, . . . the covered entity is ultimately responsible for ensuring individuals are notified[.]" *Id.*

information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate." 45 C.F.R. § 164.530(f).

2482. The MOVEit Data Breach is considered a breach under the HIPAA Rules because it involved an access of PHI not permitted under the HIPAA Privacy Rule.

2483. A breach under the HIPAA Rules is defined as "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. § 164.40.

2484. The MOVEit Data Breach resulted from a combination of insufficiencies that demonstrate that DDCA and Affiliates failed to comply with safeguards mandated by HIPAA regulations.

2485. As HIPAA covered business entities, DDCA and Affiliates are required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured PHI, as in the case of the MOVEit Data Breach.

2486. As HIPAA-covered entities handling medical patient data, DDCA and Affiliates' data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the Data Breach.

E. Delta Dental Bellwether Defendants Failed to Comply with Industry Standards

2487. Several best practices have been identified that at a minimum should be implemented by entities, like Delta Dental Bellwether Defendants, that handle highly sensitive and confidential Private Information.

2488. These best practices include, but are not limited to: educating all employees about data security practices and procedures; requiring strong passwords; implementing multi-layer security—including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

2489. Other standard cybersecurity practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

2490. On information and belief, Delta Dental Bellwether Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

2491. These foregoing frameworks are existing and applicable industry standards, and Delta Dental Bellwether Defendants failed to comply with these accepted standards, thereby opening the door to Cl0p and causing the Data Breach.

F. Had Delta Dental Bellwether Defendants Taken Their Obligations Seriously, They Would Have Determined that the MOVEit Software was not Safe to Use

2492. Delta Dental Bellwether Defendants are responsible for protecting the Private Information they solicit and collect from attacks and breaches that result from weaknesses in third-party systems and software.

2493. Delta Dental Bellwether Defendants failed to safeguard Delta Dental Bellwether Plaintiffs' and Class Members' Private Information when they failed to adopt and enforce reasonable and available data security practices and procedures to prevent and/or mitigate the known risk of a cyberattack.

2494. Prior to the Data Breach, Delta Dental Bellwether Defendants should have, but did not, implement and maintain reasonable and necessary data security policies and procedures, which would have mitigated or avoided the Data Breach.

2495. There are numerous known and available steps that Delta Dental Bellwether Defendants could have taken to mitigate or even prevent the Data Breach.

2496. Data security practices that could and should have been implemented by Delta Dental Bellwether Defendants to prevent the MOVEit Data Breach include:

a. Auditing of third-party software, including the MOVEit Transfer software;

b. Vetting and periodic auditing of third-party vendors, including Progress;

c. Restricting MOVEit transfers to pre-approved IP addresses ("whitelisting");

d. Limiting the specific types of files that can be uploaded;

e. Conducting basic monitoring of web servers;

f. Using web application firewalls ("WAFs"); and

g. Employing supply chain security.

1. Auditing Third-Party Software.

2497. Security audits of third-party software enable companies to identify vulnerabilities, monitor access to sensitive data, and discover and remediate any unauthorized data access.[689] Here,

[689] *6 Security Tips for Third Party* Software, Cybersecurity Insiders, https://www.cybersecurity-insiders.com/6-security-tips-for-third-party-software/ (last visited May 20, 2024).

security auditing of the MOVEit Transfer software could have prevented the Data Breach. The methods for conducting security audits of third-party software are well-known and widely available.[690] Delta Dental Bellwether Defendants therefore could and should have employed companies that conduct security audits of third-party software.[691]

2. Vetting Vendors.

2498. In addition to auditing third-party software, proper vetting and routine audits of vendors' data security practices, including vetting of Progress's cybersecurity practices, could have prevented the Data Breach. Vendor risk assessments or security questionnaires are "one of the best methods for extracting deep cybersecurity insights about any aspects of a vendor's attack surface."[692] Industry-standard risk assessments and security questionnaires designed to help companies discover vulnerabilities in third-party web applications and software are widely available,[693] and can be used to assess the security of third-party software against common attack vectors, including SQL injection susceptibility.[694]

3. Whitelisting.

2499. Restricting MOVEit transfers to pre-approved IP addresses—a cybersecurity practice referred to as "whitelisting"—could also have prevented the Data Breach. A whitelist is

---

[690] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard (updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software.

[691] Davit Asatryan, *Third-Party Applications Audit: Complete Guide*, Spin.ai (Nov. 4, 2021, updated Apr. 19, 2024), https://spinbackup.com/blog/third-party-applications-audit/.

[692] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard (updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software ("Risk assessments can either be framework-based to identify security control deficiencies against popular security standards or custom-designed for focused investigations about specific third-party risks.").

[693] *Id.*

[694] *Id.*

an administrator-defined register of entities pre-approved for authorized access or to perform specific actions. Whitelisting enhances the security of a system or network by ensuring that only pre-approved users or devices have access to sensitive data or systems. Whitelisting thus denies access by default, providing authorization only to a vetted, pre-approved list of IP addresses, applications, email addresses, and/or users. Blacklisting, in contrast, requires that known threats be specifically identified and blocked, while everything else is permitted. By definition, a blacklist cannot protect against an exploitation of a Zero-Day vulnerability, like the one Cl0p exploited in the MOVEit Data Breach. NIST Special Publication 800-167: *Guide to Application Whitelisting* provides specific guidance to companies on how to implement whitelisting.[695]

4. Limiting Specific File Types.

2500. Limiting the specific types of files that can be uploaded via FTP could also have prevented the Data Breach. After exploiting the MOVEit vulnerability via SQL injection, Cl0p uploaded the LEMURLOOT web shell, which masqueraded as a legitimate file[696] and allowed the threat actor to execute commands, download files, extract system settings, and create/insert/delete users.[697]

2501. Proper data security dictates that only those files that are needed and expected to be uploaded should be allowed. This typically includes document file types such as .doc, .docx, .pdf, etc. Only web site administrators with whitelisted IP addresses should have been allowed to upload web page files, such as .aspx.

---

[695] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf.

[696] https://blog.qualys.com/vulnerabilities-threat-research/2023/06/07/progress-moveit-transfer-vulnerability-being-actively-exploited; *see also* https://securityintelligence.com/news/the-moveit-breach-impact-and-fallout-how-can-you-respond/.

[697] *#StopRansomware: Cl0p Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, CISA (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

5. Adequate Logging, Monitoring, and Auditing.

2502. "Logging, monitoring, and auditing procedures help an organization prevent incidents and provide an effective response when they occur."[698] These tools can detect SQL injection attempts and mitigate or even prevent breaches like the MOVEit Data Breach.

2503. Forensic examinations of the MOVEit Data Breach have confirmed that indicators of compromise were found in the logs of targeted organizations,[699] verifying that effective log monitoring would have mitigated or even prevented the Data Breach. Accordingly, Delta Dental Bellwether Defendants could and should have utilized commonly available tools that monitor logs automatically and provide alerts of unusual activity to administrators.

2504. "Several different logs record details of activity on systems and networks. For example, firewall logs record details of all traffic that the firewall blocked. By monitoring these logs, it's possible to detect incidents. Some automated methods of log monitoring automatically detect potential incidents and report them right after they've occurred."[700]

2505. Here, adequate logging and log monitoring could have prevented the MOVEit Data Breach because logs would have shown clear indicators of compromise and/or malicious activity. SQL injection attempts, successful or not, will appear in such logs. But even extensive logging is insufficient without adequate monitoring of said logs.

---

[698] Mike Chapple, et al., (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide (9th ed. 2021).

[699] Scott Downie, et al., *Transfer Vulnerability (CVE-2023-34362) Since* 2021, Kroll (June 8, 2023), https://www.kroll.com/en/insights/publications/cyber/clop-ransomware-moveit-transfer-vulnerability-cve-2023-34362.

[700] Darril Gibson, CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide at p. 73 (2017).

2506. The U.S. National Institute of Standards and Technology (NIST) publishes a Cybersecurity Framework that emphasizes continuous monitoring of systems.[701] The NIST SP 800-92 Guide to Computer Security Log Management further defines how to manage logs,[702] and there are a number of widely available tools that can monitor logs automatically and provide alerts to administrators when there is unusual activity.

2507. Monitoring web server logs for new files, as recommended in NIST SP 800-12,[703] is a widely accepted cybersecurity practice[704] that would have promptly detected the new files introduced in the MOVEit Data Breach. Web server monitoring would have specifically allowed Delta Dental Bellwether Defendants to detect the new files introduced to the web server root (human.aspx and human2.aspx) that enabled Cl0p to perpetrate the MOVEit Data Breach. Even basic monitoring of Delta Dental Bellwether Defendants' web servers could therefore have prevented the Data Breach because it would have revealed the backdoor Cl0p introduced to the web server.[705]

---

[701] NIST, *The NIST Cybersecurity Framework (CSF) 2*.0, Nat'l Inst. of Standards and Tech. (Feb. 26, 2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[702] NIST, *Guide to Computer Security Log Management*, Nat'l Inst. of Standards and Tech. (Sept. 2006), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf.

[703] NIST, *An Introduction to Information Security*, NIST Special Publication 800-12, Rev. 1 (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

[704] *Monitor web server directories for changed / new files*, https://serverfault.com/questions/1145284/monitor-web-server-directories-for-changed-new-files (last visited May 20, 2024); *Gateway Script to monitor directory for new files*, Ignition https://forum.inductiveautomation.com/t/gateway-script-to-monitor-directory-for-new-files/16124/5 (last visited May 20, 2024).

[705] Tyler Lioi, *MOVEit Transfer Investigations*, CrowdStrike Blog (June 5, 2023), https://www.crowdstrike.com/blog/identifying-data-exfiltration-in-moveit-transfer-investigations/.

2508. In addition to file system monitoring to identify new files, the InfoSec institute recommends: (a) network monitoring to identify rogue IP addresses which may be performing malicious activities such as brute-force or fuzzing; (b) authentication monitoring to identify unusual logins or login attempts; (c) file change monitoring to identify changes to sensitive files within the file system; and (d) process monitoring to identify rogue processes that might be malicious.[706]

2509. Beyond monitoring activity, the actual data transferred via MOVEit could and should have been monitored by Delta Dental Bellwether Defendants. Most legitimate interactions utilizing MOVEit only upload or download relatively small amounts of data at a given time, but Cl0p was able to exfiltrate large amounts of consumer data in the Data Breach. Had Delta Dental Bellwether Defendants been adequately monitoring data transfers, any attempt to exfiltrate large amounts of data (significantly varying from normal usage) would have triggered an alert.

6. WAFs.

2510. Properly configured web application firewalls ("WAFs") could also have prevented or mitigated the effects of the MOVEit Data Breach.[707]

7. Supply Chain Security.

2511. Supply chain security is another common method of ensuring that all items in the supply chain, including third-party software like MOVEit, is secure.[708]

---

[706] Lester Obbayi, *Web server protection: Web server security monitoring*, InfoSec (May 4, 2020), https://www.infosecinstitute.com/resources/network-security-101/web-server-protection-web-server-security-monitoring/.

[707] *See, e.g.*, *Web Application Firewall*, Imperva, https://www.imperva.com/products/web-application-firewall-waf/ (last visited Apr. 26, 2024); Huawei Cloud, *How Does WAF Detect SQL Injection, XSS, and PHP Injection Attacks?* (Sept. 6, 2023), https://support.huaweicloud.com/intl/en-us/waf_faq/waf_01_0457.html.

[708] NIST, *Best Practices in Cyber Supply Chain Risk Management – Conference Materials*, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-

2512. The National Institute of Standards and Technology explicitly discusses vulnerabilities in third party software[709] and provides three supply chain security principles[710] that, if applied, would have mitigated or prevented the MOVEit breaches:

Figure 25

Cyber Supply Chain Security Principles:

1. **Develop your defenses based on the principle that your systems will be breached**. When one starts from the premise that a breach is inevitable, it changes the decision matrix on next steps. The question becomes not just how to prevent a breach, but how to mitigate an attacker's ability to exploit the information they have accessed and how to recover from the breach.
2. **Cybersecurity is never just a technology problem, it's a people, processes and knowledge problem**. Breaches tend to be less about a technology failure and more about human error. IT security systems won't secure critical information and intellectual property unless employees throughout the supply chain use secure cybersecurity practices.
3. **Security is Security.** There should be no gap between physical and cybersecurity. Sometimes the bad guys exploit lapses in physical security in order to launch a cyber attack. By the same token, an attacker looking for ways into a physical location might exploit cyber vulnerabilities to get access.

8. Windows Security Feature.

2513. Delta Dental Bellwether Defendants utilizing Windows have an additional protection modality. The Windows security system has ransomware protection, which allows the user to designate any folder as protected. Any attempt to add new files or change existing files in that folder would then have to be approved. Because LEMURLOOT masqueraded as a legitimate file that was then used as a backdoor, having the folder \inetpub\wwwroot\ protected from alterations would have prevented these files from being uploaded.

2514. In addition to the foregoing data security practices, which, if adopted by Delta Dental Bellwether Defendants, could have prevented the Data Breach, there are a number of common security techniques and mechanisms that should be a part of any standard data security

---

Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf (last visited Dec. 3, 2024).

[709] *Id.*

[710] *Id.*

policy and could have limited the scope of damage from a data breach. These security techniques and practices include:

a. Limiting access by employing a "least privileges" policy;

b. Implementing "zero-trust" security frameworks;

c. Encrypting data at rest; Immediately applying patches once they were made available.

2515. A "least privileges" policy can limit an attacker who exploits a vulnerability from accessing large volumes of data. Limiting access via policies such as least privileges means that, even if a threat actor is able to exploit a vulnerability or even use a legitimate login to access the system, access to sensitive data will be limited. The large volume of records accessed and exfiltrated in the Data Breach indicates that this was not done, because it is highly unlikely that any login would have legitimate access to that amount of sensitive data.

2516. "Zero Trust" is a security model and set of system design principles that emphasize security verification in network environments. The core principle of Zero Trust is "never trust, always verify." Thus, unlike traditional security models that assume everything inside a network is safe, Zero Trust assumes threats can exist both inside and outside the network.

2517. Zero Trust security frameworks require all users, whether inside or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted access to applications and data.[711] Numerous

[711] *See, e.g., Zero Trust, A revolutionary approach to Cyber or just another buzz word?*, Deloitte (2021), https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/deloitte-cyber-zero-trust.pdf; *see also* Venu Shastri, *Zero Trust Architecture*, CrowdStrike (June 28, 2023), https://www.oracle.com/security/what-is-zero-trust; https://www.crowdstrike.com/cybersecurity-101/zero-trust-security.

standards provide guidelines to organizations implementing "zero-trust" security frameworks, including NIST SP 800-207,[712] NIST SP 800-205,[713] and the CISA zero trust maturity model.[714]

2518. Two aspects of Zero Trust are particularly applicable to the MOVEit Data Breach. The first is the network is segmented into smaller, secure zones to maintain separate access for different parts of the network. This reduces the lateral movement of attackers within the network. The second is continuously monitoring the security posture of all hardware and software on the network. This helps to detect and respond to threats in real time.

2519. The United States Cybersecurity & Infrastructure Security Agency published recommendations for mitigating the MOVEit vulnerability by "[g]rant[ing] admin privileges and access only when necessary, establishing a software allow list that only executes legitimate applications."[715]

2520. Finally, following Progress's announcement of the first MOVEit vulnerability on May 31, 2023,[716] Delta Dental Bellwether Defendants should have, but did not, immediately begin taking security measures. Delta Dental Bellwether Defendants' failure to adequately safeguard Delta Dental Bellwether Plaintiffs' and Class Members' Private Information resulted in that information being accessed or obtained by third-party cybercriminals.

---

[712] NIST, *NIST SP 800-207 – Zero Trust Architecture*, CSRC (Aug. 2020), https://csrc.nist.gov/pubs/sp/800/207/final.

[713] NIST, *NIST SP 800-205 – Attribute Considerations for Access Control Systems*, CSRC (June 2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-205.pdf.

[714] *Zero Trust Maturity Model*, CISA (Apr. 2023), https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf.

[715] *#StopRansomware: Cl0p Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, CISA (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[716] *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)*, Progress: Community (June 16, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023.

G. Delta Dental Bellwether Defendants Failed to Follow Progress's Recommendations Regarding Secure Configuration Of The MOVEit Software.

2521. The MOVEit software offers secure configurations that any customer could implement to make the system more secure and to mitigate that impact of this breach.

2522. Progress made several additional recommendations to users of the MOVEit software, including:

a. Using consistency check and tamper check utilities to validate consistently and the audit log.

b. Review audit logs for any anomalous behavior. Such anomalous behavior includes:

i. Sign-ons from specific IP addresses

ii. APIs used

iii. Modification of settings

c. Limiting administrative privileges.[717]

d. IP and user lockout policies.[718]

e. Whitelisting so only specific IP addresses and users could login remotely.[719]

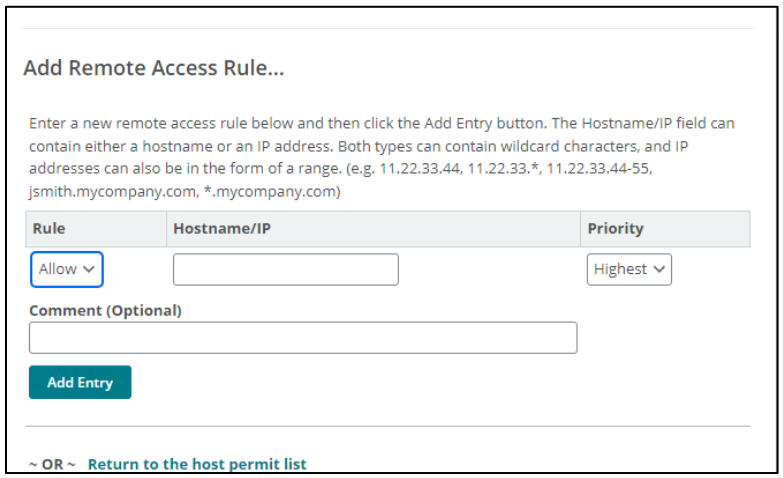
2523. Delta Dental Bellwether Defendants could and should have turned on whitelisting:

[717] *Progress Documentation: MOVEit Transfer 2022 Administrator Guide*, Progress (updated Apr. 6, 2022), https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/Permissions_3.html.

[718] *Progress Documentation: MOVEit Automation Web Admin Help – IP/User Lockout Policy*, Progress (updated Feb. 21, 2022), https://docs.progress.com/bundle/moveit-automation-web-admin-help-2022/page/IPUser-Lockout-Policy.html.

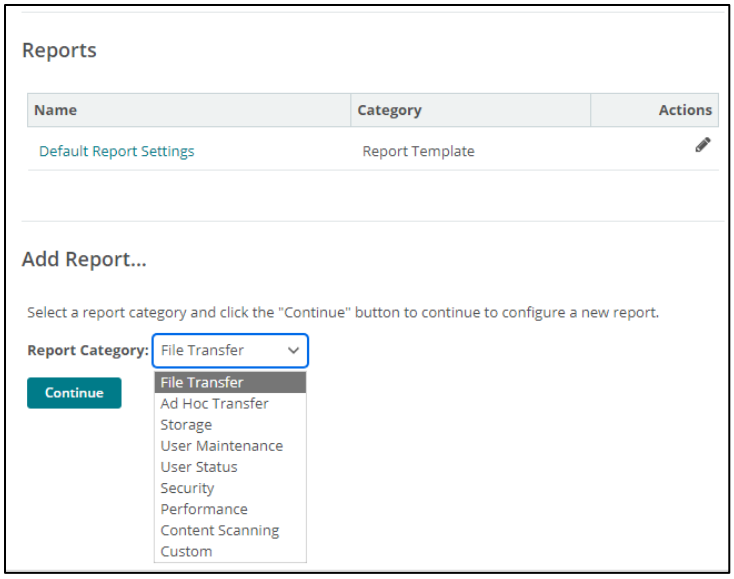
[719] *MOVEit Transfer – Whitelist IP for Specific Users Accounts*, Progress: Community (Oct. 14, 2020), https://community.progress.com/s/article/moveit-transfer-whitelist-ip-for-specific-users-accounts.

Figure 26



2524. Generating reports in MOVEit is also a simple process:

Figure 27



2525. There are a number of security reports built into the MOVEit software:

Figure 28

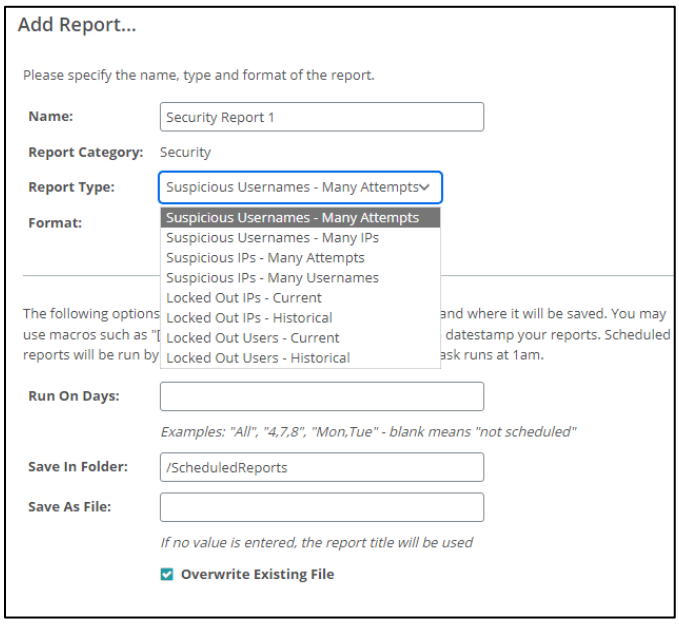
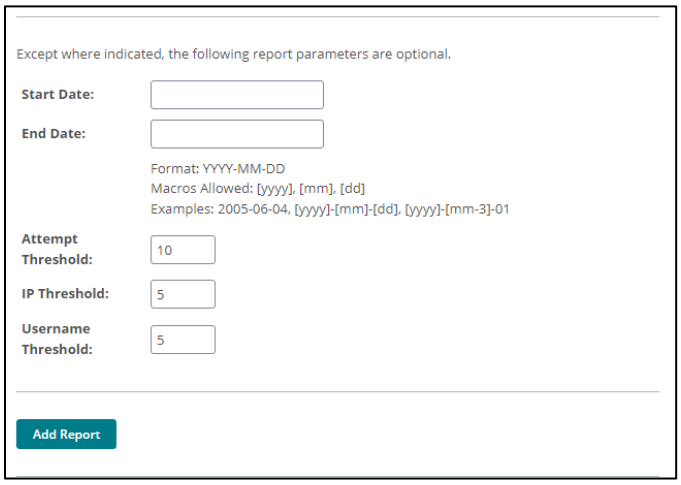
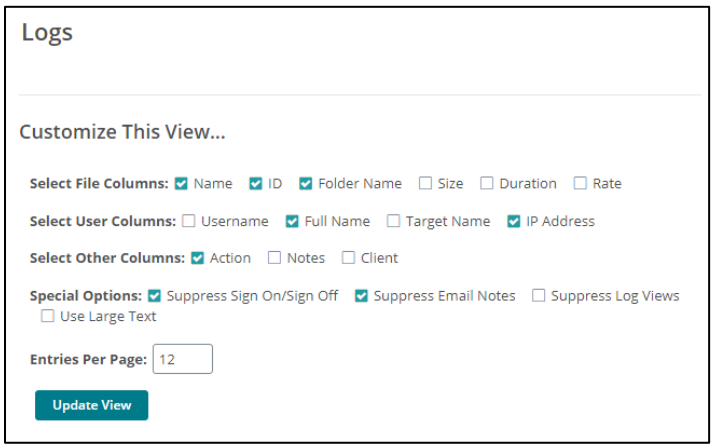


Figure 29



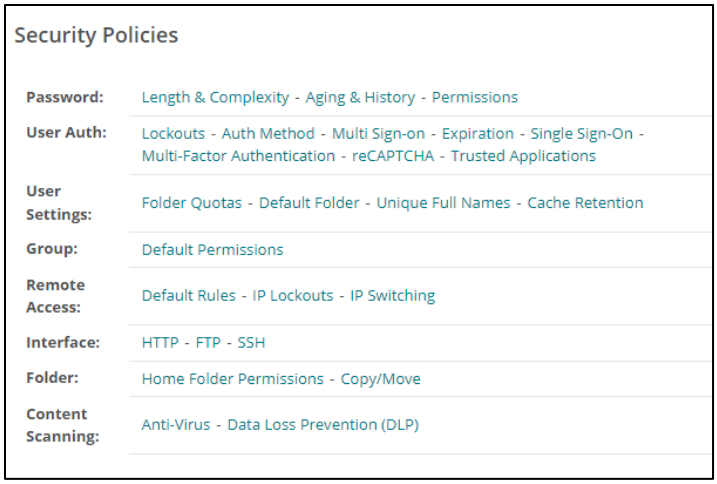
2526. MOVEit users can also customize the view of logs:

Figure 30



2527. A number of additional security policies can be set with a simple point and click:

Figure 31



2528. Data loss prevention rules could and should have been enabled to prevent exfiltration of data:

Figure 32

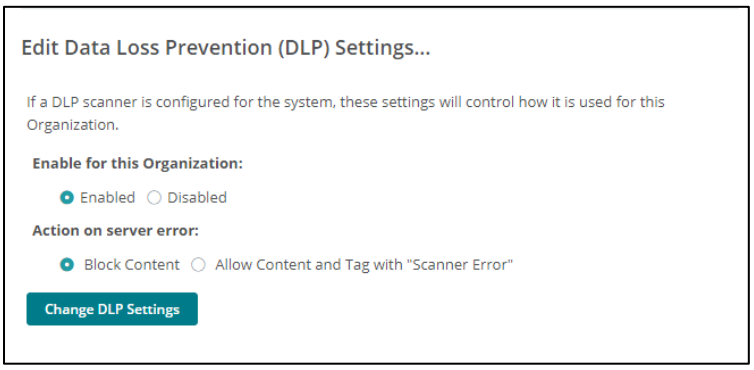


Figure 33

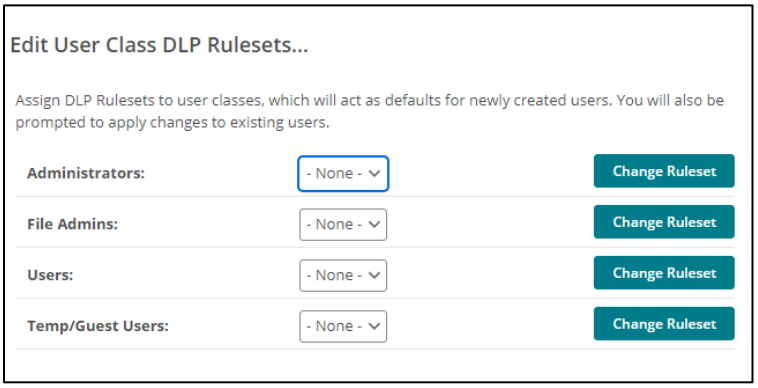
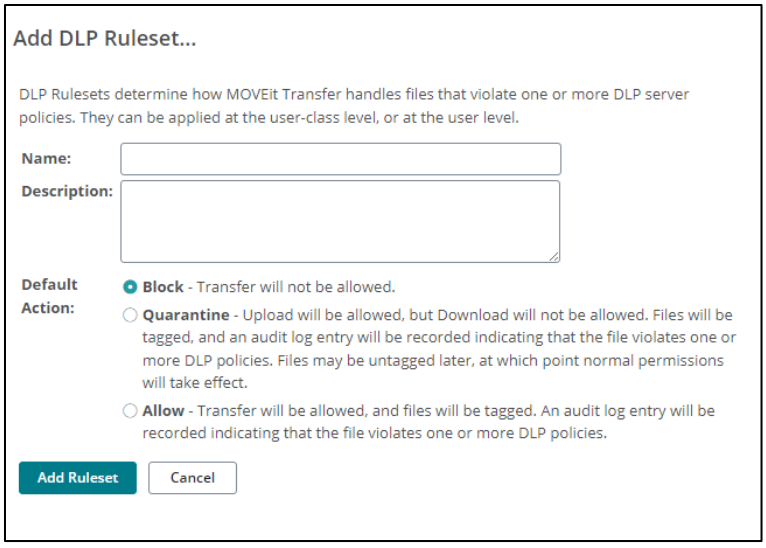


Figure 34



2529. It is unclear which, if any, of these security measures were implemented by Delta Dental Bellwether Defendants.

H. Delta Dental Bellwether Defendants Chose to Use the MOVEit Software to Transfer Sensitive Information Despite its Security Flaws

2530. Delta Dental Bellwether Defendants enriched themselves by saving the costs they reasonably should have expended on adequate data security measures to secure Delta Dental Bellwether Plaintiffs' and Class Members' Private Information.

2531. Instead of providing a reasonable level of security that would have prevented the Data Breach, Delta Dental Bellwether Defendants instead calculated to avoid their data security obligations at the expense of Delta Dental Bellwether Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Delta Dental Bellwether Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Delta Dental Bellwether Defendants' failures to provide the requisite security.

I. Delta Dental Bellwether Defendants Failed to Protect and Satisfy Their Legal Obligations

2532. Despite Delta Dental Bellwether Defendants' duty to safeguard Delta Dental Bellwether Plaintiffs' and Class Members' Private Information, Delta Dental Bellwether Defendants nevertheless employed inadequate data security measures to protect and secure the data with which they were entrusted, resulting in the Data Breach and the subsequent compromise and theft of Delta Dental Bellwether Plaintiffs' and Class Members' Private Information. As described in Chapter One, had Delta Dental Bellwether Defendants taken their obligations seriously, they would have determined that the MOVEit software was not safe and would put Delta Dental Bellwether Plaintiffs' and Class Members' Private Information at risk.

2533. Although Delta Dental Bellwether Defendants owed a non-delegable duty to Delta Dental Bellwether Plaintiffs and Class Members to implement reasonable and adequate security measures to protect their Private Information, they maintained, stored, disclosed, shared, and/or transferred their Private Information in a negligent and/or reckless manner. In particular, Delta

Dental Bellwether Plaintiffs' and Class Members' Private Information was maintained on computer systems in a condition vulnerable to cyberattacks.

2534. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Delta Dental Bellwether Plaintiffs' and Class Members' Private Information was a known risk to Delta Dental Bellwether Defendants, and thus they were on notice that failing to take steps necessary to ensure their vendors or their business associates' vendors, including Progress, with whom they shared Private Information, properly safeguarded Delta Dental Bellwether Plaintiffs' and Class Members' Private Information from those risks left the Private Information in a vulnerable condition.

2535. As alleged in this Complaint, as well as in Chapter One, DDCA and Affiliates failed to comply with HIPAA and HITECH, including in the following ways:

a. Failing to maintain adequate security practices, systems, and protocols to prevent data loss and theft;

b. Failing to mitigate risks of data breach and implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. 164.308(a)(1);

c. Failing to ensure the confidentiality, integrity, and protection of electronic PHI that DDCA and Affiliates create, receive, maintain, and transmit in violation of 45 C.F.R. 164.306(a)(1).

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. 164.308(a)(6)(ii);

g. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. 164.306(a)(2);

h. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendants' workforce in violation of 45 C.F.R. 164.306(a)(4);

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. 164.502, *et seq*.; and

k. Retaining information past a recognized purpose and not deleting it.

l. Failing to ensure that their third-party vendor, Progress, had implemented adequately safe and secure policies and practices.

2536. As discussed above, DDCA and Affiliates failed to comply with FTC guidelines and industry standards as well. *See also* Chapter One and Chapter Two.

2537. Similarly, DDA failed to comply with HIPAA and HITECH, including in the following ways:

a. Failing to maintain adequate security practices, systems, and protocols to prevent data loss and theft;

b. Failing to mitigate risks of data breach and implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. 164.308(a)(1);

c. Failing to ensure the confidentiality, integrity, and protection of electronic PHI that they create, receive, maintain, and/or transmits in violation of 45 C.F.R. 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. 164.308(a)(6)(ii);

g. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. 164.306(a)(2);

h. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. 164.306(a)(3);

i. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. 164.502, *et seq*.; and

j. Retaining information past a recognized purpose and not deleting it.

2538. Delta Dental Companies in DDA's network have historically been subject to numerous data breaches[720] during which unauthorized agents gained access to their or their vendors' network systems, compromising the Private Information of their customers. As described herein, DDCA and Affiliates knew based on breaches of Delta Dental Companies' networks and the prevalence of cyberattacks across the industry that the data they collected and stored was highly valuable and vulnerable. *See* Chapter One and Chapter Two.

2539. Although DDA disclosed that the MOVEit Transfer servers that were the target of the Data Breach were located within the Delta Dental of California network environment, the details otherwise of the Data Breach remain in the exclusive control of Delta Dental Bellwether Defendants. For example, Delta Dental Bellwether Defendants did not disclose the ways in which they failed to comply with data security regulations and industry standards that made them

[720] *See, e.g.*, "Important Security Event Notice" (breach of Delta Dental of Washington's own network systems) (2022), notice available here: https://perma.cc/DH99-EUEF (last visited Jun. 4, 2024); "Notice of EyeMed Vision Care LLC Data Breach" (vendor of Delta Dental affiliate) (2020), notice available here: https://perma.cc/QT25-3A9N (last visited Jun. 4, 2024).

vulnerable to the Data Breach, by way of their third-party service provider, MOVEit, or otherwise. Moreover, although DDCA and Affiliates admitted to Delta Dental Bellwether Plaintiffs that their "health insurance information" and "treatment cost information" had been compromised, DDCA and Affiliates failed to indicate, for example, whether the data included the treatment itself, *i.e.*, the medical condition, which is of utmost sensitivity – and public disclosure of which could lead to humiliation or other serious harms.

2540. However, upon information and belief, Delta Dental Bellwether Defendants breached their duties and obligations in one or more of the following ways, by: (i) failing to design, test, implement, monitor, and maintain reasonable software and/or network safeguards against foreseeable threats; (ii) failing to design, implement, and maintain reasonable data retention policies; (iii) failing to adequately train staff on data security; (iv) failing to comply with industry-standard data security practices; (v) failing to warn Delta Dental Bellwether Plaintiffs and Class Members of inadequate data security practices; (vi) failing to adequately encrypt the Private Information; (vii) failing to adequately secure decryption keys so that they could not be accessed by unauthorized users; and (viii) otherwise failing to secure the software and hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

2541. As part of Delta Dental Bellwether Defendants' investigation into the Data Breach, Delta Dental Bellwether Defendants' cybersecurity team reached out to Progress with specific questions about MOVEit's encryption and decryption process. Delta conceded it was using an earlier version (2020.1) of MOVEit. Delta's questions focused in particular on where and how MOVEit stored the encryption keys. In addition, Delta Dental Bellwether Defendants' cybersecurity team asked specifically about the decryption process, including when MOVEit

decrypts the files, if at any time other than during transit; where MOVEit pulls the encryption key from as part of the decryption process; and what other mechanisms (if any) are involved in the decryption process, including the database, application, or other MOVEit technology.

2542. By July 2023, Delta Dental Bellwether Defendants had analyzed the Data Breach and identified specific recommendations that could be implemented to further improve their security posture. Delta Dental Bellwether Defendants reached out to Progress to discuss their recommendations, as they had potential impacts to both the MOVEit application and Progress's own support and/or warranty considerations.

2543. Additionally, after confirming on July 6, 2023 that the Data Breach affected DDCA and Affiliates' data, DDCA and Affiliates failed to comply with the Breach Notification Rule by waiting an unreasonable amount of time, far longer than the permissible 60-day limit, to disclose the Data Breach to their customers through "individual notifications,"[721] in violation of their duties as covered entities. 45 C.F.R. §§ 164.400-414.

J. DDCA and Affiliates Waited Over Five Months to Notify Delta Dental Bellwether Plaintiffs and Class Members After Discovering the Data Breach

2544. As described Chapter One and Chapter Two and realleged herein, Progress's MOVEit software was the target of a catastrophic and devastating successful cyberattack that affected thousands of its clients and compromised the Private Information of millions of their and their clients' customers, including almost seven million customers of the Delta Dental insurance

[721] *See* 45 C.F.R. § 164.404 Notification to individuals. *Breach Notification Rule*, https://perma.cc/KM4C-F3FR (last visited Jun. 4, 2024) ("These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach."); *see, e.g.*, Data Breach Notifications, Office of the Maine Attorney General; Copy of notice to affected Maine residents: "AG Notice – ME – Delta Dental + Affiliates," PDF available for download here: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/4d61e15b-a303-4653-8206-9d54aa0d1e26.shtml (last visited Dec. 4, 2024) (demonstrating DDCA delayed more than 60 days to notify impacted individuals).

member companies within DDA's network whose Private Information was stored or otherwise in use on the MOVEit Transfer servers located within the Delta Dental of California network environment.

2545. The victims of the Data Breach were subject to the highly offensive disclosure of their Private Information. Specifically, the Private Information included "names with some combination of the following: addresses, Social Security numbers, driver's license numbers or other state identification numbers, passport numbers, financial account information, tax identification numbers, individual health insurance policy numbers, and/or health information."[722]

2546. The "Notice of Data Security Incident" (hereafter "Notice Letter") was sent and signed by "Delta Dental of California and affiliates" with the address listed as 560 Mission Street, Suite 1300, San Francisco, CA 94105. The Notice Letter defines "Delta Dental of California and affiliates" as follows therein:

> "The Delta Dental of California enterprise includes its affiliates Delta Dental Insurance Company; Delta Dental of the District of Columbia, Delta Dental of Delaware, Inc., Delta Dental of Pennsylvania, Delta Dental of New York, Inc., Delta Dental of West Virginia, and their affiliated companies, as well as the national DeltaCare USA network."

2547. Delta Dental Bellwether Plaintiffs and Class Members all received a Notice Letter from "Delta Dental of California and affiliates[,]" rather than from the Delta Dental Company through which they purchased insurance.

2548. DDCA and Affiliates waited over five months after discovering the breach to begin to send their customers Notice Letters that their data had been compromised. In the Notice Letter,

[722] Data Breach Notifications, Office of the Maine Attorney General; Copy of notice to affected Maine residents: "AG Notice – ME – Delta Dental + Affiliates," PDF available for download here: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/4d61e15b-a303-4653-8206-9d54aa0d1e26.shtml (last visited Dec. 4, 2024).

Delta Dental of California and affiliates admit to Delta Dental Bellwether Plaintiffs' and Class Members' that they were victims of a data breach, finally revealing to them that their highly sensitive, personal data was accessed by an unauthorized third party and compromised. They disclosed as follows:[723]

a. "Delta Dental of California and affiliates ('Company') experienced a data security incident involving the MOVEit Transfer ('MOVEit') software, an application used by our company and many organizations worldwide."

b. "On June 1, 2023, the Company learned unauthorized actors exploited a vulnerability affecting the MOVEit file transfer software application."

c. "On July 6, 2023, our investigation confirmed that Company information on the MOVEit platform had been accessed and acquired without authorization between May 27, 2023 and May 30, 2023. At that time, we promptly engaged independent third-party experts in computer forensics, analytics, and data mining to determine what information was impacted and with whom it is associated."

2549. Delta Dental of California and affiliates admitted to each recipient that "[on] November 27, 2023, [it] determined [their] personal information was affected."

2550. Upon information and belief, Delta Dental of California and affiliates sent its first batch of notifications to its customers who were victims of the Data Breach that their data had been compromised on December 14, 2023 – the date that the Notice of Security Incident was sent to the Maine Office of Attorney's General.[724]

2551. In other words, Delta Dental of California and affiliates waited, *at minimum*, six and a half months after learning about the unauthorized activity on the MOVEit Platform (June 1, 2023) before it revealed this crucial information to its customers and suggested that they start

[723] *Id.*

[724] *Id.*

taking precautions to protect their identities, *e.g.*, merely review their credit reports, or to offer them identity monitoring services due to the risks they now faced as a result of the Data Breach.

2552. Even after concluding its own investigation and confirming that its customers' personal identifying and personal health information had been compromised on July 6, 2023, Delta Dental of California and affiliates still waited, *at minimum*, nearly five and a half months before it started notifying its customers directly of the breach and potential risks they faced as a result.[725]

2553. However, most of the Delta Dental Bellwether Plaintiffs' Notice Letters, *see infra*, are dated after January 23, 2024 and up to as late as February 9, 2024—in other words, almost eight months after Delta Dental of California and affiliates learned about the breach, and almost two and a half months after identifying on November 27, 2023 that the Delta Dental Bellwether Plaintiffs' own Private Information was compromised.

2554. When Delta Dental of California and affiliates finally sent notice to its customers about the Data Breach, it deliberately underplayed the Data Breach's severity and obscured the nature of the Data Breach. For example, the Notice Letter fails to explain how the breach occurred (what security weakness was exploited), what exact data elements of each affected individual were compromised, who the Data Breach was perpetrated by, and the extent to which those data elements were compromised. Delta Dental of California and affiliates claims that after learning about the breach on June 1, 2023 it "enhanced unauthorized access monitoring related to MOVEit Transfer file access, malicious activity, and ransomware activity[]" but does not specify how its steps actually mitigate the harms caused by the Data Breach or describe how these measures will prevent further breaches, nor its ability to protect Delta Dental Bellwether Plaintiffs' and Class

[725] "Delta Dental of California Data Breach: 7 Million Individuals Affected." THE HIPAA JOURNAL, published Dec. 17, 2023, available here: https://perma.cc/WZE9-R483 (last visited Jun. 4, 2024).

Members' Private Information from future unauthorized disclosure, as required by HIPAA, 45 C.F.R. § 164.404.

2555. In the Notice Letter, Delta Dental of California and affiliates also claims that "[d]ata security is a priority []. We apply security patches for known vulnerabilities provided by third-party software vendors, regularly update our capabilities to monitor potential security threats and consistently manage access to our systems and data."[726] Notably, this statement appears after informing the recipient what of their data was compromised, in the "What Are We Doing" section, along with its offer of a free 24 months of identity monitoring services. Thus, it is ambiguous as to whether these are new measures in place, *i.e.*, what Delta Dental of California and affiliates is now doing as a result of the breach, or whether these were security measures already in place. Delta Dental of California and affiliates does not offer any assurances or indication that these measures are reasonable or adequate to safeguard and protect Delta Dental Bellwether Plaintiffs' and Class Members' Private Information in the future or whether Delta Dental Bellwether Plaintiffs and Class Members remain vulnerable to new attacks.

2556. Delta Dental of California and affiliates' offer of 24 months of identity monitoring services is woefully inadequate given the lifetime – not merely two years – of risks Delta Dental Bellwether Plaintiffs and Class Members now face as a result of the Data Breach.

2557. Delta Dental of California and affiliates' offer itself indicates that it recognizes that Delta Dental Bellwether Plaintiffs and Class Members are at a present and continuing risk of identity theft and fraud as a result of the Data Breach, and that these risks arose once Delta Dental of California and affiliates confirmed the breach, back in July 2023—when Delta Dental of

[726] *See* Delta Dental, *Notice of Data Breach*, https://perma.cc/ESW4-SFHX (last visited Jun. 4, 2024).

California and affiliates first confirmed that Delta Dental of California and affiliates' data had been impacted. Yet Delta Dental of California and affiliates has offered no measures to protect Delta Dental Bellwether Plaintiffs and Class Members from these lifetime risks they now face, and upon information and belief, have failed to offer relief for the damages they suffered due to its own negligence that left Delta Dental Bellwether Plaintiffs' and Class Members' Private Information vulnerable to attack and theft.

2558. Delta Dental of California and affiliates merely "encourage[d] individuals to remain vigilant by reviewing bank accounts, credit reports and other financial statements closely and immediately reporting any suspicious activity to the company that maintains the account for the individual."[727] In the Notice Letter, it suggested Delta Dental Bellwether Plaintiffs and Class Members run credit reports, place a security freeze on their accounts, set up fraud alerts, and report any suspicious activity. In other words, Delta Dental of California and affiliates shifted the burden to Delta Dental Bellwether Plaintiffs and Class Members to remediate their own harms and be responsible for preventing future harms.

2559. As alleged, DDCA and Affiliates' unreasonable delay in notifying their customers of the Data Breach was in violation of their obligations as "covered entities" under the HIPAA Breach Notification Rule, 45 C.F.R. § 164.404. Moreover, by failing to notify Delta Dental Bellwether Plaintiffs and Class Members that their Private Information may have been compromised as early as July, DDCA and Affiliates prevented Delta Dental Bellwether Plaintiffs and Class Members from taking reasonable precautions to try to mitigate the harms of the Data

[727] Data Breach Notifications, Office of the Maine Attorney General; Copy of notice to affected Maine residents: "AG Notice – ME – Delta Dental + Affiliates," PDF available for download here: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/4d61e15b-a303-4653-8206-9d54aa0d1e26.shtml (last visited Dec. 4, 2024).

Breach, in violation of 45 C.F.R. § 164.530(f), which required DDCA and Affiliates, as covered entities, to mitigate the harmful effects of the Data Breach. To the contrary, by waiting over five months to notify affected individuals, DDCA and Affiliates exacerbated the harmful effects and risks to Delta Dental Bellwether Plaintiffs and Class Members caused by the Data Breach.

K. Delta Dental Bellwether Plaintiffs and Class Members Suffered Serious Harms

2560. As alleged and incorporated herein, as victims of a cybercriminal data breach, Delta Dental Bellwether Plaintiffs and Class Members face immediate and significant harm. *See* Chapter One and Chapter Two.

2561. As alleged and incorporated herein, Delta Dental Bellwether Plaintiffs and Class Members suffered injuries in numerous ways and are at risk of future injuries for the rest of their lives. *See* Chapter One and Chapter Two.

2562. As a direct and proximate result of Delta Dental Bellwether Defendants' collective wrongful actions and inaction and the resulting Data Breach, Delta Dental Bellwether Plaintiffs and Class Members have already been harmed by the fraudulent misuse of their Private Information, and have been placed at an imminent, immediate, and continuing increased risk of additional harm from identity theft and identity fraud, requiring them to put time which they otherwise would have dedicated to other life demands such as work and family into an effort to mitigate both the actual and potential impact of the Data Breach on their lives. Such mitigatory actions include, *inter alia*, closely reviewing and monitoring their credit reports and accounts for unauthorized activity; investigating suspicious, unauthorized activity in their financial accounts or credit; placing "freezes" and "alerts" with credit reporting agencies; contacting their financial institutions, reversing charges, closing or modifying financial accounts; sorting through dozens of

phishing and spam email, text, and phone communications. This time has been lost forever and cannot be recaptured.

2563. Delta Dental Bellwether Defendants' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Delta Dental Bellwether Plaintiffs' and Class Members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft and misuse of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and misused via the sale of Delta Dental Bellwether Plaintiffs' and Class Members' information on the Internet's black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their Private Information;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. ascertainable losses in the form of deprivation of the value of their Private Information, for which there is a well-established national and international market;

h. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach; and

i. nominal damages

2564. While Delta Dental Bellwether Plaintiffs' and Class Members' Private Information has been stolen, Defendants continue to hold Delta Dental Bellwether Plaintiffs' and Class Members' Private Information. Particularly because Defendants have demonstrated an inability to

prevent a breach or stop it from continuing even after being detected, Delta Dental Bellwether Plaintiffs and Class Members have an undeniable interest in ensuring that their Private Information is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

2565. Delta Dental Bellwether Plaintiffs and Class Members have suffered from the unauthorized disclosure of their Private Information. The disclosure of their Social Security numbers and their protected health information in particular is highly offensive due to the sensitivity of the private and personal data and severely consequential, accompanied by various harmful uses of their Private Information that identity thieves capitalize on. *See* Chapter One and Chapter Two.

II. CLASS ALLEGATIONS

2566. Delta Dental Bellwether Plaintiffs bring this class action behalf of themselves and, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) as representatives of the following classes:

DDA Nationwide Class

All persons who provided their Private Information to DDA whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDA.

DDA California Class

All residents of California who provided their Private Information to DDA whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDA.

DDA Connecticut Class

All residents of Connecticut who provided their Private Information to DDA whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDA.

DDA Florida Class

All residents of Florida who provided their Private Information to DDA whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDA.

DDA Georgia Class

All residents of Georgia who provided their Private Information to DDA whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDA.

DDA Iowa Class

All residents of Iowa who provided their Private Information to DDA whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDA.

DDA New York Class

All residents of New York who provided their Private Information to DDA whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDA.

DDA Pennsylvania Class

All residents of Pennsylvania who provided their Private Information to DDA whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDA.

DDA South Carolina Class

All residents of South Carolina who provided their Private Information to DDA whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDA.

DDA Tennessee Class

All residents of Tennessee who provided their Private Information to DDA whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDA.

DDA Texas Class

All residents of Texas who provided their Private Information to DDA whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDA.

DDCA Nationwide Class

All persons whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA.

DDCA California Class

All residents of California whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA.

DDCA Connecticut Class

All residents of Connecticut whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA.

DDCA Georgia Class

All residents of Georgia whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA.

DDCA Florida Class

All residents of Florida whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA.

DDCA Iowa Class

All residents of Iowa whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA.

DDCA New York Class

All residents of New York whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA.

DDCA Pennsylvania Class

All residents of Pennsylvania whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA.

DDCA South Carolina Class

All residents of South Carolina whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA.

DDCA Tennessee Class

All residents of Tennessee whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA.

DDCA Texas Subclass

All residents of Texas whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA.

DDIC Nationwide Class

All persons who provided their Private Information to DDIC whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDIC.

DDIC Connecticut Class

All residents of Connecticut who provided their Private Information to DDIC whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDIC.

DDIC Florida Class

All residents of Florida who provided their Private Information to DDIC whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDIC.

DDIC Georgia Class

All residents of Georgia who provided their Private Information to DDIC whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDIC.

DDIC Iowa Class

All residents of Iowa who provided their Private Information to DDIC whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDIC.

DDIC South Carolina Class

All residents of South Carolina who provided their Private Information to DDIC whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDIC.

DDIC Texas Class

All residents of Texas who provided their Private Information to DDIC whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDIC.

DDNY Nationwide Class

All persons who provided their Private Information to DDNY whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDNY.

DDNY New York Class

All residents of New York who provided their Private Information to DDNY whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDNY.

DDPenn Nationwide Class

All persons who provided their Private Information to DDPenn. whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDPenn.

DDPenn Georgia Class

All residents of Georgia who provided their Private Information to DDPenn. whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDPenn.

DDPenn New York Class

All residents of New York who provided their Private Information to DDPenn. whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDPenn.

DDPenn Pennsylvania Class

All residents of Pennsylvania who provided their Private Information to DDPenn. whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDPenn.

DDPenn Texas Class

All residents of Texas who provided their Private Information to DDPenn. whose Private Information was compromised in the MOVEit Data Breach where such Private Information was obtained from or hosted by DDCA and/or DDPenn.

2567. All of the foregoing classes are referred to in this Chapter, collectively, as the "Delta Dental Bellwether Class." The Nationwide DDA, DDCA, DDIC, DDNY, and DDPenn Classes are collectively referred to as the "Delta Dental Bellwether Nationwide Classes." The DDA State Classes, DDCA State Classes, DDIC State Classes, DDNY NY Class, and DDPenn State Class (i.e., all state classes alleged in the Delta Dental Chapter) are collectively referred to as the "Delta Dental State Classes."

2568. Excluded from the foregoing classes are: (1) the judges presiding over the action; (2) the Defendants, their subsidiaries, parent companies, successors, predecessors, and any entity in which Defendants or their parents have a controlling interest, and their current or former officers and directors; (3) persons who properly opt out; and (4) the successors or assigns of any such excluded persons.

2569. **Numerosity**: Class Members are so numerous that their individual joinder is impracticable, as the proposed Class includes at least 6,928,932 members who are geographically dispersed.

2570. **Typicality**: Delta Dental Bellwether Plaintiffs' claims are typical of Delta Dental Bellwether Class Members' claims. Delta Dental Bellwether Plaintiffs and all Delta Dental Bellwether Class Members were injured through Delta Dental Bellwether Defendants' uniform misconduct, and Delta Dental Bellwether Plaintiffs' claims are identical to the claims of the Delta Dental Bellwether Class Members they seek to represent.

2571. **Adequacy**: Delta Dental Bellwether Plaintiffs' interests are aligned with those of the Delta Dental Bellwether Class Members they seek to represent, and Delta Dental Bellwether

Plaintiffs have retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Delta Dental Bellwether Plaintiffs and their counsel intend to prosecute this action vigorously. All Delta Dental Bellwether Class Members' interests are well-represented by Delta Dental Bellwether Plaintiffs and undersigned counsel.

2572. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Delta Dental Bellwether Plaintiffs' and other Delta Dental Bellwether Class Members' claims. The injury suffered by each individual Delta Dental Bellwether Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Delta Dental Bellwether Class Members individually to effectively redress Delta Dental Bellwether Defendants' wrongdoing. Even if Delta Dental Bellwether Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, an economy of scale, and comprehensive supervision by a single court.

2573. **Commonality and Predominance:** The following questions common to all Delta Dental Bellwether Class Members predominate over any potential questions affecting individual Delta Dental Bellwether Class Members:

a. Whether Delta Dental Bellwether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information from unauthorized access and disclosure;

b. Whether Delta Dental Bellwether Defendants failed to exercise reasonable care to secure and safeguard Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information;

c. Whether Delta Dental Bellwether Defendants breached their duties to protect Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information;

d. Whether Delta Dental Bellwether Defendants violated the statutes alleged herein;

e. Whether Delta Dental Bellwether Plaintiffs and all other Delta Dental Bellwether Class Members are entitled to damages and the measure of such damages and relief.

2574. Given that Delta Dental Bellwether Defendants engaged in a common course of conduct as to Delta Dental Bellwether Plaintiffs and all other Delta Dental Bellwether Class Members, similar or identical injuries and common law violations are involved, and common questions outweigh any potential individual questions.

III. CAUSES OF ACTION

DELTA DENTAL BELLWETHER FIRST CLAIM FOR RELIEF
Negligence

(On Behalf of the Delta Dental Nationwide Classes, or in the alternative, the Delta Dental Bellwether State Classes)

2575. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2576. Delta Dental Bellwether Plaintiffs bring this claim against DDA on behalf of the DDA Nationwide Class, or, in the alternative, the DDA State Classes. In addition, the Delta Dental Bellwether Plaintiffs bring this claim against DDCA on behalf of the DDCA Nationwide Class, or, in the alternative, the DDCA State Classes. Delta Dental Bellwether Plaintiffs Karen Boginski, Doris Cadet, John Meeks, Terrill Mendler, Manuel Mendoza, and Yvette Tillman (collectively, the "DDIC Bellwether Plaintiffs") bring this claim against DDIC on behalf of the DDIC

Nationwide Class or, in the alternative, the DDIC State Classes. Delta Dental Bellwether Plaintiff Michelle Gonsalves brings this claim against DDNY on behalf of the DDNY Nationwide Class or, in the alternative, the DDNY NY Class. Delta Dental Bellwether Plaintiffs Marvin Dovberg, Margaret Kavanagh, Diamond Roberts, and Taneisha Robertson (collectively, the "DDPenn Bellwether Plaintiffs") bring this claim against DDPenn on behalf of the DDPenn Nationwide Class, or, in the alternative, the DDPenn State Classes.

2577. Delta Dental Bellwether Defendants require their customers to submit non-public Private Information as a condition of becoming a customer and receiving dental insurance.

2578. Delta Dental Bellwether Defendants gathered and stored the Private Information of Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members as part of their businesses, which affects commerce.

2579. As customers of DDCA and Affiliates, Delta Dental Bellwether Plaintiffs and Delta Dental Class Members, or their dentalcare providers, continue to send DDCA and Affiliates new Private Information as they receive care, *e.g.*, related to treatments and costs.

2580. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members entrusted Delta Dental Bellwether Defendants with their Private Information with the reasonable understanding that their highly personal Private Information would be safeguarded and protected against unauthorized disclosure.

2581. As part of their business operations, DDCA and Affiliates, as governed by HIPAA agreements, shared that information with Defendant DDA.

2582. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members reasonably believed they were entrusting DDA with their Private Information as well, given that Delta Dental Bellwether Plaintiffs could access their Private Information related to their Delta

Dental insurance through their DDA account, on the DDA website— branded identically to other Delta Dental Bellwether Defendants' respective websites. Moreover, to sign up for an account on DDA's webpage or request information about insurance claims or coverage, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members were required to input their Private Information.

2583. Delta Dental Bellwether Defendants had full knowledge of the high monetary value and sensitivity of Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information and the types of harm that Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members could and would suffer if their Private Information was wrongfully disclosed.

2584. Delta Dental Bellwether Defendants owed a duty of care to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

2585. By assuming the responsibility to collect and store this data, as well as sharing it and utilizing it to derive business value and commercial profits, DDCA and Affiliates owed a duty under common law to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information and keep it from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

2586. These duties extended to Defendant DDA, which holds itself out to the public, including to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members, through its website, as being responsible for "employ[ing] reasonable safeguards designed to

promote the security of our systems and protect your personal information from unauthorized destruction, use, modification, or disclosure" across its 39 dental insurance membership companies, which include the other Delta Dental Bellwether Defendants. DDA also utilizes their Private Information for commercial profits. Additionally, customers of DDCA and Affiliates can sign up for an account on DDA's website which requires them to disclose their Private Information. They can request Private Information related to coverage or claims through DDA directly, which also requires them to disclose Private Information.

2587. Delta Dental Bellwether Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

2588. Delta Dental Bellwether Defendants purport to be trusted providers of dental insurance. Delta Dental Bellwether Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Delta Dental Bellwether Defendants, on the one hand, and Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members, on the other hand. That special relationship arose because of DDCA and Affiliates' businesses as providers of dental insurance, which required Delta Dental Bellwether Plaintiffs and Class Members to provide and entrust DDCA and Affiliates with their confidential Private Information to receive dental insurance.

2589. Thus, Delta Dental Bellwether Defendants were in a unique and superior position to protect against the harm suffered by Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members as a result of the Data Breach.

2590. Delta Dental Bellwether Defendants owed a duty to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members to select a software file transfer service that employed reasonable data security measures to protect their customers' Private Information.

2591. The risk that unauthorized persons would attempt to gain access to Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information and misuse was foreseeable to all Delta Dental Bellwether Defendants. They had a common law duty to prevent foreseeable harm to others because Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Delta Dental Bellwether Defendants. By collecting, receiving, storing, and using Private Information that is routinely targeted by criminals for unauthorized access, they were obligated to act with reasonable care to protect against these foreseeable threats.

2592. Delta Dental Bellwether Defendants knew, or should have known, the importance of exercising reasonable care in handling the Private Information entrusted to them.

2593. Delta Dental Bellwether Defendants' Privacy Policies acknowledge their duties to adequately protect the personal and medical information of Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members in accordance with the law.

2594. Delta Dental Bellwether Defendants had a duty to promptly and adequately notify Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members about the Data Breach, but failed to do so, and breached this duty.

2595. Delta Dental Bellwether Defendants had and continue to have duties to adequately disclose that Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information within Delta Dental Bellwether Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was and continues to be necessary to allow Delta Dental Bellwether Plaintiffs and the Delta Dental Bellwether Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

2596. Delta Dental Bellwether Defendants breached their duties owed to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members and thus were negligent. Delta Dental Bellwether Defendants breached these duties by, among other things: (a) mismanaging their systems and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of Private Information; (b) mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to detect the breach at the time it began or within a reasonable time thereafter; and (f) failing to follow its own policies and practices published to its clients.

2597. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach and harms suffered.

2598. Delta Dental Bellwether Defendants' respective negligent conduct is ongoing, in that Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information remains in Delta Dental Bellwether Defendants' possession in an unsafe and insecure manner.

2599. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members are entitled to injunctive relief requiring Delta Dental Bellwether Defendants to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Delta Dental Bellwether Class Members.

DELTA DENTAL BELLWETHER SECOND CLAIM FOR RELIEF
Negligence *Per Se*
(On Behalf of the Delta Dental Nationwide Classes, or in the alternative, the Delta Dental Bellwether State Classes)

2600. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2601. Delta Dental Bellwether Plaintiffs bring this claim against DDA on behalf of the DDA Nationwide Class, or, in the alternative, the DDA State Classes. In addition, the Delta Dental Bellwether Plaintiffs bring this claim against DDCA on behalf of the DDCA Nationwide Class, or, in the alternative, the DDCA State Classes. The DDIC Bellwether Plaintiffs bring this claim against DDIC on behalf of the DDIC Nationwide Class or, in the alternative, the DDIC State Classes. Plaintiff Michelle Gonsalves brings this claim against DDNY on behalf of the DDNY Nationwide Class or, in the alternative, the DDNY NY Class. The DDPenn Bellwether Plaintiffs bring this claim against DDPenn on behalf of the DDPenn Nationwide Class, or, in the alternative, the DDPenn State Classes. Delta Dental Bellwether Defendants had duties arising under HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and the FTC Act to protect Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information.

2602. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Delta Dental Bellwether Defendants, of failing to use reasonable measures to protect sensitive consumer data, including Private Information.

2603. Various FTC publications and orders promulgated pursuant to the FTC Act also form the basis of Delta Dental Bellwether Defendants' duty.

2604. Delta Dental Bellwether Defendants breached their duties, pursuant to the FTC Act and other applicable standards, and thus were negligent, by failing to implement fair, reasonable, or appropriate computer systems and data security practices that complied with applicable industry standards to safeguard Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information as part of its business practices.

2605. Under HIPAA, DDCA and Affiliates are "covered entities" and DDA is a "business associates."

2606. DDCA and Affiliates' duty to use reasonable security measures under HIPAA required them to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l).

2607. DDCA and Affiliates owed a duty to "reasonably safeguard protected health information from any intentional or unintentional use or disclosure." 45 C.F.R. § 164.530(c)(2). Some or all of the healthcare and/or medical information that was compromised and stolen constitutes "protected health information" within the meaning of HIPAA. 42 U.S.C. § 1320d(6); 45 C.F.R. § 160.103.

2608. As a business associate, DDA also owed these legal obligations to implement administrative, technical, and physical safeguards. 42 U.S. Code § 17931 (applying security requirements to business associates and incorporating security requirements into BAAs between business associates and covered entities); *see also* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards); 42 U.S.C. § 17902.[728]

[728] "The HITECH Act Summary;" https://perma.cc/HSQ6-4942 (last visited Jun. 4, 2024).

2609. By waiting over five months to notify affected individuals, Delta Dental Bellwether Defendants exacerbated the harmful effects and risks to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members caused by the Data Breach, in violation of 45 C.F.R. § 164.530(f).

2610. Delta Dental Bellwether Defendants' specific negligent acts and omissions, resulting in failure to comply with HIPAA and HITECH regulations include, but are not limited to, the following: (i) failing to adopt, implement, and maintain adequate security measures to safeguard Delta Dental Bellwether Class Members' Private Information; (ii) failing to adequately monitor the security of their networks and systems; (iii) allowing unauthorized access to Delta Dental Bellwether Class Members' Private Information; (iv) failing to detect in a timely manner that Delta Dental Bellwether Class Members' Private Information had been compromised; (v) failing to remove former employees' Private Information they were no longer required to retain pursuant to regulations; and (vi) failing to timely and adequately notify Delta Dental Bellwether Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

2611. Delta Dental Bellwether Defendants' violations of HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and Section 5 of the FTC Act (and similar state statutes) independently constitute negligence *per se*.

2612. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members are consumers within the class of persons that HIPAA, HITECH, and Section 5 of the FTC Act were intended to protect.

2613. The harms that have occurred are the types of harm HIPAA, HITECH, and the FTC Act were intended to guard against.

2614. The FTC has pursued enforcement actions against businesses and healthcare entities that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harms as those suffered by Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members.

2615. In addition, under various state data security and consumer protection statutes such as those outlined herein, Delta Dental Bellwether Defendants had a duty to implement and maintain reasonable security procedures and practices to safeguard Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information.

2616. Delta Dental Bellwether Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored, the high frequency of cyber-attacks that target the exact type of Private Information targeted here, and the foreseeable consequences of a data breach of that nature.

2617. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members were foreseeable victims of Delta Dental Bellwether Defendants' violations of HIPAA, HITECH, and the FTC Act, and state data security and consumer protection statutes. Delta Dental Bellwether Defendants knew or should have known that their failure to implement reasonable data security measures to protect and safeguard Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information would cause damage to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members.

2618. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members were foreseeable victims of Delta Dental Bellwether Defendants' negligent acts and omissions. Delta Dental Bellwether Defendants knew or should have known that their failure to implement reasonable data security measures to protect and safeguard Delta Dental Bellwether Plaintiffs' and

Delta Dental Bellwether Class Members' Private Information would cause damage to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members.

2619. Delta Dental Bellwether Defendants violated their own policies by failing to maintain the confidentiality of Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' records; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information, and ultimately disclosing Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information.

2620. DDA violated its BAAs with each of the other Delta Dental Bellwether Defendants under which it agreed to protect customers, including Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' PHI, and were subject to privacy and security safeguard requirements and standards established by HIPAA, HITECH, and the Omnibus Rule.

2621. But for Delta Dental Bellwether Defendants' violations of the applicable laws and regulations, Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information would not have been accessed by unauthorized parties.

2622. As a direct and proximate result of Delta Dental Bellwether Defendants' negligence *per se*, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members have suffered and will continue to suffer injuries, including, but not limited to: (i) theft of their Private Information; (ii) costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts; (iii) costs associated with purchasing credit monitoring and identity theft protection services; (iv) lowered credit scores resulting from credit inquiries following fraudulent activities; (v) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future

consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts; (vi) the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals; (vii) damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Delta Dental Bellwether Defendants with the mutual understanding that they would safeguard Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' data against theft and not allow access and misuse of their data by others; (viii) continued and certainly increased risk of exposure to hackers and thieves of their Private Information, and additional unauthorized viewing of their Private Information that was already hacked in the Data Breach; (ix) loss of their privacy and confidentiality in their Private Information; (x) the erosion of the essential and confidential relationship with their dental insurance provider, which used Progress's software and exposed them to these privacy risks, or their dental network, DDA, a business associate of their dental provider; (xi) loss of personal time and opportunity costs to monitor and/or remedy harms caused by theft of their Private Information; (xii); an increase in spam calls, texts, and/or emails; and (xiii) the continued and certainly increased risk to their Private Information.

2623. As a direct and proximate result of Delta Dental Bellwether Defendants' negligence *per se*, Delta Dental Bellwether Plaintiffs and the Delta Dental Bellwether Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

2624. Finally, as a direct and proximate result of Delta Dental Bellwether Defendants' negligence *per se*, Delta Dental Bellwether Plaintiffs and the Delta Dental Bellwether Class have

suffered and will suffer the continued risks of exposure of their Private Information, which remains in DDCA and Affiliates' possession and is subject to further unauthorized disclosures so long as Delta Dental Bellwether Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

DELTA DENTAL BELLWETHER THIRD CLAIM FOR RELIEF
Breach Of Implied Contract
(On Behalf of the Delta Dental Nationwide Classes, or in the alternative, the Delta Dental Bellwether State Classes)

2625. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2626. Delta Dental Bellwether Plaintiffs bring this claim against DDA on behalf of the DDA Nationwide Class, or, in the alternative, the DDA State Classes. In addition, the Delta Dental Bellwether Plaintiffs bring this claim against DDCA on behalf of the DDCA Nationwide Class, or, in the alternative, the DDCA State Classes. The DDIC Bellwether Plaintiffs bring this claim against DDIC on behalf of the DDIC Nationwide Class or, in the alternative, the DDIC State Classes. Plaintiff Michelle Gonsalves brings this claim against DDNY on behalf of the DDNY Nationwide Class or, in the alternative, the DDNY NY Class. The DDPenn Bellwether Plaintiffs bring this claim against DDPenn on behalf of the DDPenn Nationwide Class, or, in the alternative, the DDPenn State Classes. Delta Dental Bellwether Defendants solicited, offered, and invited Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members to provide their Private Information as part of their regular business practices in exchange for dental insurance.

2627. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members were required to, and did, provide their Private Information to DDCA and Affiliates in exchange

for the provision of dental insurance. As alleged herein, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members also provided their Private Information to DDA.

2628. The mutual understanding and intent of Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members on the one hand, and Delta Dental Bellwether Defendants on the other, is demonstrated by their conduct and course of dealing. Delta Dental Bellwether Defendants required Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members to provide their Private Information as a condition of services. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members accepted the offers for services and complied.

2629. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members paid DDCA and Affiliates for dental insurance.

2630. All Delta Dental Bellwether Defendants accepted Delta Dental Bellwether Plaintiffs' and Class Members' Private Information, whether directly from them, or through their contracts with other Delta Dental Bellwether Defendants.

2631. Delta Dental Bellwether Defendants relied on for their businesses, and conferred direct and indirect monetary benefits from, the Private Information provided by Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members and thus from Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members themselves, and had full knowledge of the benefits they conferred.

2632. In providing their Private Information to Delta Dental Bellwether Defendants and paying DDCA and Affiliates for dental insurance, and all Delta Dental Bellwether Defendants accepting that Private Information, directly or indirectly, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members conferred a direct benefit on them, and entered into

implied contracts with Delta Dental Bellwether Defendants by which the Delta Dental Bellwether Defendants agreed to keep such information secure and confidential, ensure protection of the Private Information from unauthorized access or disclosure, and to timely and adequately notify Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members if their data had been breached and compromised or stolen.

2633. Upon accepting Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information, DDCA and Affiliates provided Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information to DDA in their ordinary course of business as member companies of DDA's dental insurance network.

2634. Upon accepting Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information, DDA shared Private Information with DDCA and Affiliates.

2635. Privacy Policies and Practices of Delta Dental Bellwether Defendants assure Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members of their shared practices to safeguard Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information and of their legal obligations to do so.

2636. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members entered these same implied contracts with DDA whose web platform targets new or existing customers, such as Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members, holding itself out as part of the same brand of dental insurance providers, and inviting them to learn more about and sign up for dental insurance through one of its 39 Delta Dental Companies, which include DDCA and Affiliates, or to create an account, input Private Information, and request information about their personal insurance claims. Based on their interactions alone with DDA, and/or their special and business relationship with DDCA and Affiliates, Delta Dental Bellwether

Plaintiffs and Delta Dental Bellwether Class Members could reasonably (and correctly) believe that the Delta Dental Company from which they purchased dental insurance exchanged data with DDA, and they could also reasonably believe that DDA and their Delta Dental insurance provider were one and the same. For these reasons, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members would have reasonable expectations around privacy and security of their Private Information shared with DDA, just as they had of the other Delta Dental Bellwether Defendants.

2637. Delta Dental Bellwether Defendants accepted and maintained the Private Information of Delta Dental Bellwether Plaintiffs and the Delta Dental Bellwether Class that they acquired either from one another, as governed by HIPAA agreements, or direct receipt from Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members, and thus monetarily benefitted from Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members providing their Private Information. Thus, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members entered into implied contracts with DDCA and Affiliates' business associates, revenue service providers, and file transfer software providers, including DDA.

2638. Alternatively, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members were the intended beneficiaries of Business Associate Agreements entered into between DDCA and Affiliates and their business associates, including DDA, which governed use, disclosure, and transfer terms of their Private Information.

2639. In entering into these implied contracts, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members reasonably believed and expected that Delta Dental Bellwether Defendants' data security practices complied with relevant laws and regulations and

were consistent with industry standards, and that they would thoroughly vet and select vendors that adequately protected Private Information.

2640. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members would not have entrusted their Private Information to Delta Dental Bellwether Defendants in the absence of implied contracts between them that they would keep, and require the third-party vendors they select to store, transfer, and use their Private Information in fair, secure, reasonable, and legally compliant ways.

2641. Implicit in these agreements between Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members and Delta Dental Bellwether Defendants were Delta Dental Bellwether Defendants' obligations to: (a) take reasonable steps to safeguard that Private Information, including through proper vetting of third party vendors to whom Private Information is provided; (b) prevent unauthorized disclosure of the Private Information; (c) provide Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information; (d) reasonably safeguard and protect the Private Information of Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members from unauthorized disclosure or uses; and (e) retain or allow third parties to retain Private Information only under conditions that kept such information secure and confidential.

2642. Delta Dental Bellwether Defendants breached the implied contracts they entered into with Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members by failing to safeguard and protect their Private Information. These failures include entrusting their Private Information to a vendor that fails to safeguard Private Information; failing to delete the Private Information of Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members

from their own databases or requiring vendors to delete Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information once they are no longer customers of DDCA and Affiliates and users of DDA's platform; and failing to provide accurate notice to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members that their Private Information was compromised as a result of the Data Breach so that they could take prompt and adequate precautions to mitigate the risks caused by the Data Breach.

2643. Moreover, implied in these exchanges was a promise by Delta Dental Bellwether Defendants to ensure that the Private Information of Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members was only used in connection with the agreed-upon healthcare services.

2644. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members therefore did not receive the benefit of their bargains, because they provided their Private Information in exchange for an implied agreement by Delta Dental Bellwether Defendants to keep it safe and secure within its computer systems and network environment; in addition to DDCA and Affiliates' and DDA's implied agreement to keep it safe and secure in connection with sharing Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information under their BAAs and providing it to third-party vendors, under distinct BAAs.

2645. Delta Dental Bellwether Defendants' conduct and lax security unfairly interfered with Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' rights to receive the full benefit of their contracts.

2646. Had Delta Dental Bellwether Defendants disclosed to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members that they did not have security practices to secure sensitive data, including adequate policies to verify the security of their third-party vendors

or business associates, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members would not have provided their Private Information to Delta Dental Bellwether Defendants, and thus would not have entered into implied contracts with Delta Dental Bellwether Defendants.

2647. As a direct and proximate result of Delta Dental Bellwether Defendants' breaches, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain and overpaying for dental insurance.

2648. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

2649. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members are also entitled to injunctive relief requiring Delta Dental Bellwether Defendants to, *e.g.*, (i) strengthen their data monitoring procedures; (ii) evaluate, audit, and improve their processes for vetting third party vendors and the selection processes for vendors to which Delta Dental Bellwether Defendants provide sensitive Private Information; (iii) submit to future annual audits of those systems and monitoring procedures; and (iv) immediately provide or continue providing adequate credit monitoring to all Class Members.

DELTA DENTAL BELLWETHER FOURTH CLAIM FOR RELIEF
Breach Of Implied Covenant Of Good Faith And Fair Dealing
(On Behalf of the Delta Dental Nationwide Classes, or in the alternative, the Delta Dental Bellwether State Classes)

2650. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2651. Delta Dental Bellwether Plaintiffs bring this claim against DDA on behalf of the DDA Nationwide Class, or, in the alternative, the DDA State Classes. In addition, the Delta Dental Bellwether Plaintiffs bring this claim against DDCA on behalf of the DDCA Nationwide Class, or, in the alternative, the DDCA State Classes. The DDIC Bellwether Plaintiffs bring this claim against DDIC on behalf of the DDIC Nationwide Class or, in the alternative, the DDIC State Classes. Plaintiff Michelle Gonsalves brings this claim against DDNY on behalf of the DDNY Nationwide Class or, in the alternative, the DDNY NY Class. The DDPenn Bellwether Plaintiffs bring this claim against DDPenn on behalf of the DDPenn Nationwide Class, or, in the alternative, the DDPenn State Classes. As alleged, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members entered into implied contracts with Delta Dental Bellwether Defendants when they provided and entrusted them with their Private Information in exchange for the provision of dental insurance. In doing so, Delta Dental Bellwether Plaintiffs and the Delta Dental Bellwether Class entered into implied contracts with Delta Dental Bellwether Defendants by which they agreed to safeguard and protect such information to keep such information secure and confidential, and to timely and accurately notify Delta Dental Bellwether Plaintiffs and the Delta Dental Bellwether Class if their data had been breached and compromised or stolen.

2652. Privacy Policies and Practices of Delta Dental Bellwether Defendants assure Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members of their shared practices to safeguard Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information and of their legal obligations to do so under HIPAA.

2653. While Delta Dental Bellwether Defendants had discretion in the specifics of how they met applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing that is inherent in every contract.

2654. Delta Dental Bellwether Defendants breached this implied covenant of good faith and fair dealing when they engaged in acts and/or omissions that are declared unfair trade practices by the FTC, HIPAA, HITECH, and state statutes and regulations. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information; selection of and providing Private Information to a vendor that does not adequately safeguard Private Information; and failing to disclose to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members at the time they provided their Private Information to Delta Dental Bellwether Defendants that their security systems and those of their vendors, *e.g.*, Progress, failed to meet applicable legal and industry standards.

2655. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members did all or substantially all of the significant things that the contract required them to do. Likewise, all conditions required for Delta Dental Bellwether Defendants' performance were met.

2656. Delta Dental Bellwether Defendants' acts and omissions unfairly interfered with Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' rights to receive the full benefit of their contracts.

2657. As a direct and proximate result of Delta Dental Bellwether Defendants' above-alleged breach of implied contract, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members have suffered and/or will suffer harms including but not limited to: (a) actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; (b) the loss of the value of their privacy and the confidentiality of the stolen Private Information; (c) the illegal sale of the compromised Private Information on the black market; (d) the ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in

monetary loss and economic harm; (e) the mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; (f) the time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; (g) the expenses incurred and time spent initiating fraud alerts; (h) the resulting decrease in credit scores; (i) their lost work time; (j) the lost value of their Private Information; (k) the lost value of access to their Private Information permitted by Delta Dental Bellwether Defendants; (l) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Data Breach; (m) the lost benefit of their bargains (price premium damages in the form of overpayment for dental insurance); and (n) nominal and general damages; and other economic and non-economic harms.

2658. Accordingly, Delta Dental Bellwether Plaintiffs and the Delta Dental Bellwether Class are entitled to damages in an amount to be determined at trial, including actual, consequential, and nominal damages, along with costs and attorneys' fees incurred in this action.

DELTA DENTAL BELLWETHER FIFTH CLAIM FOR RELIEF
Breach Of Confidence
(On Behalf of the Delta Dental Nationwide Classes, or in the alternative, the Delta Dental Bellwether State Classes)

2659. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2660. Delta Dental Bellwether Plaintiffs bring this claim against DDA on behalf of the DDA Nationwide Class, or, in the alternative, the DDA State Classes. In addition, the Delta Dental Bellwether Plaintiffs bring this claim against DDCA on behalf of the DDCA Nationwide Class, or, in the alternative, the DDCA State Classes. The DDIC Bellwether Plaintiffs bring this claim against DDIC on behalf of the DDIC Nationwide Class or, in the alternative, the DDIC State

Classes. Plaintiff Michelle Gonsalves brings this claim against DDNY on behalf of the DDNY Nationwide Class or, in the alternative, the DDNY NY Class. The DDPenn Bellwether Plaintiffs bring this claim against DDPenn on behalf of the DDPenn Nationwide Class, or, in the alternative, the DDPenn State Classes. Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information constitutes confidential and unique information. Indeed, Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Social Security numbers can be changed only with great difficulty and time spent, which still enables a threat actor or cybercriminal to exploit that information during the interim. Private medical information, once disclosed and in the hands of identity thieves, can cause irreparable harm and humiliation, and even lead to blackmail.

2661. Delta Dental Bellwether Defendants were fully aware of the confidential and sensitive nature of Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information at all points in which they interacted with Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members thus made an implied promise of confidentiality to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members by accepting their Private Information.

2662. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state or federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

2663. By collecting and storing Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information and using it for commercial gain, Delta Dental

Bellwether Defendants undertook a duty of care to use reasonable means to secure and safeguard this Private Information to prevent disclosure and guard against its theft.

2664. As alleged herein, Delta Dental Bellwether Defendants' relationships with Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members were governed by terms and expectations that Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information would be collected, stored, and protected in confidence—by Delta Dental Bellwether Defendants and the vendors to which DDCA and Affiliates, specifically, provide that Private Information—and would not be disclosed to unauthorized third parties.

2665. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members provided their respective Private Information to DDCA and Affiliates, which are all companies within the DDA national network. DDA entered into BAAs with DDCA and Affiliates which govern the transfer and disclosure of protected health information between the parties, including requiring DDA, to abide by the HIPAA Security Rule.

2666. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members may sign up for an account directly with DDA, upon which they are required to provide their Private Information, and use its platform, for example, to request information about their insurance claims, which requires them to provide DDA with additional personal and medical related information. DDA then works with Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' individual Delta Dental Company, i.e., the individual's dental insurance, to respond.

2667. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members provided Delta Dental Bellwether Defendants with their Private Information with the explicit and

implicit understandings that Delta Dental Bellwether Defendants would protect and not permit the Private Information to be disseminated to any unauthorized parties.

2668. Due to Delta Dental Bellwether Defendants' failure to protect Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information, or retain vendors that protect the Private Information, Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' confidence, and without their express permission.

2669. As a direct and proximate cause of Delta Dental Defendants' actions and/or omissions, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members have suffered damages as alleged herein.

2670. But for the disclosure of Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information, in violation of the parties' mutual understanding of confidence including that Delta Dental Defendants would only provide Private Information to trusted vendors that adequately safeguard the information, Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information, as well as the resulting damages.

2671. The disclosure of Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information, and provision of Private Information to a vendor that does not adequately secure Private Information, constitute violations of Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' implicit agreements and understandings

that Delta Dental Bellwether Defendants would safeguard and protect their confidential and unique Private Information.

2672. The concrete injury and harm that Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members suffered was the reasonably foreseeable result of Delta Dental Bellwether Defendants' failure to ensure protection of their Private Information.

2673. As a direct and proximate result of Delta Dental Bellwether Defendants' conduct, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members have suffered or will suffer concrete injury, including, but not limited to: (a) actual identity theft; (b) the loss of the opportunity to determine how and when their Private Information is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Private Information, which remains in DDCA and Affiliates' possession and is subject to further unauthorized disclosures; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, and repair the impact of the Private Information compromised as a direct and traceable result of the Data Breach for the remainder of the lives of Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members; and (h) nominal damages.

2674. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members seek actual and nominal damages for these harms.

DELTA DENTAL BELLWETHER SIXTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of the Delta Dental Nationwide Classes, or in the alternative, the Delta Dental Bellwether State Classes)

2675. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2676. Delta Dental Bellwether Plaintiffs bring this claim against DDA on behalf of the DDA Nationwide Class, or, in the alternative, the DDA State Classes. In addition, the Delta Dental Bellwether Plaintiffs bring this claim against DDCA on behalf of the DDCA Nationwide Class, or, in the alternative, the DDCA State Classes. The DDIC Bellwether Plaintiffs bring this claim against DDIC on behalf of the DDIC Nationwide Class or, in the alternative, the DDIC State Classes. Plaintiff Michelle Gonsalves brings this claim against DDNY on behalf of the DDNY Nationwide Class or, in the alternative, the DDNY NY Class. The DDPenn Bellwether Plaintiffs bring this claim against DDPenn on behalf of the DDPenn Nationwide Class, or, in the alternative, the DDPenn State Classes. Delta Dental Bellwether Plaintiffs bring this claim for relief in the alternative to their breach of implied contract claim against Delta Dental Bellwether Defendants.

2677. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members conferred a monetary benefit on Delta Dental Defendants in connection with obtaining dental insurance, specifically providing them with their Private Information. In exchange, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members should have received from Delta Dental Defendants the services or benefits that were the subject of the transaction, and should have had their Private Information protected with adequate data security.

2678. DDCA and Affiliates would be unable to engage in their regular course of business without that Private Information, and they accepted the monetary benefits Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members provided.

2679. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members also conferred a monetary benefit on DDA, both directly and indirectly, to which DDCA and Affiliates sent Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information under the terms of Business Associate Agreements. DDA would also be unable to engage in their regular course of business without that Private Information and they accepted the monetary benefits from the provision of Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information.

2680. All Delta Dental Bellwether Defendants knew that Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members conferred a benefit upon them and accepted and retained those benefits by accepting, retaining, and using the Private Information entrusted to them. Delta Dental Bellwether Defendants profited from Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' retained data and used Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information for business purposes.

2681. Acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Delta Dental Bellwether Defendants to retain that benefit without payment of the value thereof. Specifically, Delta Dental Bellwether Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Delta Dental Bellwether Defendants instead calculated to increase their own profits at the expense of

Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members by utilizing cheaper, ineffective security measures. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members, on the other hand, suffered as a direct and proximate result of Delta Dental Bellwether Defendants' decisions to prioritize their own profits over the requisite data security.

2682. Delta Dental Bellwether Defendants failed to secure Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information and, therefore, did not fully compensate Delta Dental Bellwether Plaintiffs or Delta Dental Bellwether Class Members for the value that their Private Information provided.

2683. Because Delta Dental Bellwether Defendants failed to implement appropriate data management and security measures, under the principles of equity and good conscience, it would be unjust if Delta Dental Bellwether Defendants were permitted to retain the monetary benefit belonging to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members.

2684. Delta Dental Bellwether Defendants acquired the Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

2685. If Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members had known that Delta Dental Bellwether Defendants had not secured their Private Information, they would not have agreed to provide their Private Information to Delta Dental Bellwether Defendants.

2686. Had Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members known that Delta Dental Bellwether Defendants did not and would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their

Private Information, they would not have entrusted Delta Dental Bellwether Defendants with their Private Information.

2687. As a direct and proximate result of Delta Dental Bellwether Defendants' conduct, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to determine for themselves how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information and diminution of its value; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in DDCA and Affiliates' possession and is subject to further unauthorized disclosures so long as Delta Dental Bellwether Defendants fail to undertake appropriate and adequate measures to protect Private Information in their continued possession; (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members; (viii) emotional distress, anxiety, and inconvenience; (ix) irreparable breach of confidence in their insurance providers; (x) loss of benefit of the bargain (price premium damages in the form of overpayment for dental insurance).

2688. As a direct and proximate result of Delta Dental Bellwether Defendants' conduct, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members have suffered and

will continue to suffer other forms of injury and/or harm. It would be inequitable for the Delta Dental Bellwether Defendants to retain the benefits without paying fair value for them.

2689. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members are entitled to restitution and/or damages from Delta Dental Bellwether Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Delta Dental Bellwether Defendants from their wrongful conduct, as well as return of their sensitive Private Information and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members may seek restitution or compensation.

2690. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members may not have an adequate remedy at law against Delta Dental Bellwether Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

DELTA DENTAL BELLWETHER SEVENTH CLAIM FOR RELIEF
Invasion Of Privacy (Public Disclosure Of Private Facts)
(On Behalf of the Delta Dental Nationwide Classes, or in the alternative, the Delta Dental Bellwether State Classes)

2691. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2692. Delta Dental Bellwether Plaintiffs bring this claim against DDA on behalf of the DDA Nationwide Class, or, in the alternative, the DDA State Classes. In addition, the Delta Dental Bellwether Plaintiffs bring this claim against DDCA on behalf of the DDCA Nationwide Class, or, in the alternative, the DDCA State Classes. The DDIC Bellwether Plaintiffs bring this claim against DDIC on behalf of the DDIC Nationwide Class or, in the alternative, the DDIC State

Classes. Plaintiff Michelle Gonsalves brings this claim against DDNY on behalf of the DDNY Nationwide Class or, in the alternative, the DDNY NY Class. The DDPenn Bellwether Plaintiffs bring this claim against DDPenn on behalf of the DDPenn Nationwide Class, or, in the alternative, the DDPenn State Classes. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members reasonably expected that the highly personal, sensitive Private Information entrusted to Delta Dental Bellwether Defendants, directly or indirectly, would be kept private, confidential, and secure and would not be disclosed to any unauthorized third party or for any improper purpose.

2693. Delta Dental Bellwether Defendants unlawfully invaded the privacy rights of Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members by:

a. Failing to adequately secure their sensitive Private Information from disclosure to unauthorized third parties or for improper purposes;

b. Enabling the disclosure of personal and sensitive facts and information about them in a manner highly offensive to a reasonable person; and

c. Enabling the disclosure of their personal and sensitive Private Information without their informed, voluntary, affirmative, and clear consent.

2694. Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information, such as health information and Social Security numbers that was publicized due to the Data Breach, was highly sensitive, private, confidential, and of no general public interest, and a reasonable person would consider its publication highly offensive and egregious.

2695. A reasonable person would find it highly offensive that Delta Dental Bellwether Defendants, having collected Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' sensitive Private Information, directly or indirectly, in a commercial transaction, failed to protect such Private Information from unauthorized disclosure to third parties.

2696. In failing to adequately protect Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' sensitive Private Information, Delta Dental Bellwether Defendants

acted in reckless disregard of Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' privacy rights. Delta Dental Bellwether Defendants knew or should have known that their ineffective security measures, including the failure to verify and validate the security practices of their vendor, Progress, and the foreseeable consequences thereof, are highly offensive to a reasonable person in Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' position.

2697. Delta Dental Bellwether Defendants violated Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' right to privacy under common law.

2698. Delta Dental Bellwether Defendants' unlawful invasions of privacy damaged Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members. As a direct and proximate result of Delta Dental Bellwether Defendants' unlawful invasion of privacy and public disclosure of private facts, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members' reasonable expectations of privacy were frustrated and defeated. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out-of-pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in DDCA and Affiliates' possession, and which is subject to further breaches, so long as Delta Dental Bellwether Defendants fail to undertake

appropriate and adequate measures to protect Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information.

2699. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach and these invasions of privacy.

2700. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members are also entitled to injunctive relief requiring Delta Dental Bellwether Defendants to, *inter alia*: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to Delta Dental Bellwether Plaintiffs and Class Members.

DELTA DENTAL BELLWETHER EIGHTH CLAIM FOR RELIEF
Invasion Of Privacy (Intrusion Upon Seclusion)
(On Behalf of the Delta Dental Nationwide Classes, or in the alternative, the Delta Dental Bellwether State Classes)

2701. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2702. Delta Dental Bellwether Plaintiffs bring this claim against DDA on behalf of the DDA Nationwide Class, or, in the alternative, the DDA State Classes. In addition, the Delta Dental Bellwether Plaintiffs bring this claim against DDCA on behalf of the DDCA Nationwide Class, or, in the alternative, the DDCA State Classes. The DDIC Bellwether Plaintiffs bring this claim against DDIC on behalf of the DDIC Nationwide Class or, in the alternative, the DDIC State Classes. Plaintiff Michelle Gonsalves brings this claim against DDNY on behalf of the DDNY Nationwide Class or, in the alternative, the DDNY NY Class. The DDPenn Bellwether Plaintiffs bring this claim against DDPenn on behalf of the DDPenn Nationwide Class, or, in the alternative,

the DDPenn State Classes. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members had a reasonable expectation of privacy in the Private Information that Delta Dental Bellwether Defendants failed to safeguard and allowed to be accessed by way of the Data Breach.

2703. Delta Dental Bellwether Defendants' conduct as alleged above intruded upon Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' seclusion under common law.

2704. By intentionally and/or knowingly failing to keep Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Delta Dental Bellwether Defendants intentionally invaded Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' privacy by:

a. Intentionally and substantially intruding into Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' private affairs in a manner that identifies Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members.

2705. Delta Dental Bellwether Defendants knew that an ordinary person in Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' positions would consider Delta Dental Bellwether Defendants' intentional actions highly offensive and objectionable.

2706. Delta Dental Bellwether Defendants invaded Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members' right to privacy and intruded into Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' seclusion by intentionally

failing to safeguard, misusing, and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

2707. Delta Dental Bellwether Defendants intentionally concealed from Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members an incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

2708. As a proximate result of such intentional misuse and disclosures, Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' reasonable expectations of privacy in their Private Information were unduly frustrated and thwarted.

2709. Delta Dental Bellwether Defendants' conduct amounted to a substantial and serious invasion of Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' protected privacy interests, causing anguish and suffering such that an ordinary person would consider Delta Dental Bellwether Defendants' intentional actions or inaction highly offensive and objectionable.

2710. In failing to protect Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Delta Dental Bellwether Defendants acted with intentional malice and oppression and in conscious disregard of Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' rights to have such information kept confidential and private.

2711. As a direct and proximate result of Delta Dental Bellwether Defendants' public disclosure of private facts, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the

materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) loss of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in DDCA and Affiliates' possession, and which is subject to further breaches, so long as Delta Dental Bellwether Defendants, including DDA, fail to undertake appropriate and adequate measures to protect Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information

2712. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

DELTA DENTAL BELLWETHER NINTH CLAIM FOR RELIEF
Bailment
(On Behalf of the Delta Dental Nationwide Classes, or in the alternative, the Delta Dental Bellwether State Classes)

2713. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2714. Delta Dental Bellwether Plaintiffs bring this claim against DDA on behalf of the DDA Nationwide Class, or, in the alternative, the DDA State Classes. In addition, the Delta Dental Bellwether Plaintiffs bring this claim against DDCA on behalf of the DDCA Nationwide Class, or, in the alternative, the DDCA State Classes. The DDIC Bellwether Plaintiffs bring this claim against DDIC on behalf of the DDIC Nationwide Class or, in the alternative, the DDIC State Classes. Plaintiff Michelle Gonsalves brings this claim against DDNY on behalf of the DDNY

Nationwide Class or, in the alternative, the DDNY NY Class. The DDPenn Bellwether Plaintiffs bring this claim against DDPenn on behalf of the DDPenn Nationwide Class, or, in the alternative, the DDPenn State Classes. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members provided Private Information to Defendants, and Delta Dental Bellwether Defendants were under a duty to keep that information private and confidential.

2715. Delta Dental Bellwether Defendants received this information from Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members either directly or through their dental/healthcare providers and their business associates or one of the Delta Dental companies under a BAA.

2716. Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information is personal property, and was conveyed to Delta Dental Bellwether Defendants for the certain purpose of keeping the information private and confidential.

2717. Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information has value and is highly prized by hackers and criminals. Delta Dental Bellwether Defendants were aware of the risks they took when accepting the Private Information for safeguarding and assumed the risk voluntarily.

2718. Once Delta Dental Bellwether Defendants accepted Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information, they were in the exclusive possession of that information, and neither Delta Dental Bellwether Plaintiffs nor Delta Dental Bellwether Class Members could control that information once it was within the possession, custody, and control of Delta Dental Bellwether Defendants.

2719. Delta Dental Bellwether Defendants did not safeguard Delta Dental Bellwether Plaintiffs' or Delta Dental Bellwether Class Members' Private Information when they failed to adopt and enforce adequate security safeguards to prevent the known risk of a cyberattack.

2720. Delta Dental Bellwether Defendants' failure to safeguard Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information resulted in that information being accessed or obtained by third-party cybercriminals.

2721. As a result of Delta Dental Bellwether Defendants' failure to keep Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information secure, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members suffered injury, for which compensation— including nominal damages and compensatory damages—are appropriate.

DELTA DENTAL BELLWETHER TENTH CLAIM FOR RELIEF
Breach Of Third-Party Beneficiary Contract
(On Behalf of the DDCA Nationwide Class, or, in the alternative, DDCA State Classes; the DDIC Nationwide Class, or, in the alternative, the DDIC State Classes; the DDNY Nationwide Class, or, in the alternative, the DDNY State Classes; and the DDPenn Nationwide Class, or, in the alternative, the DDPenn State Classes)

2722. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2723. Delta Dental Bellwether Plaintiffs bring this claim against DDCA on behalf of the DDCA Nationwide Class, or, in the alternative, the DDCA State Classes. In addition, the DDIC Bellwether Plaintiffs bring this claim against DDIC on behalf of the DDIC Nationwide Class or, in the alternative, the DDIC State Classes. Plaintiff Michelle Gonsalves brings this claim against DDNY on behalf of the DDNY Nationwide Class or, in the alternative, the DDNY NY Class. The DDPenn Bellwether Plaintiffs bring this claim against DDPenn on behalf of the DDPenn

Nationwide Class, or, in the alternative, the DDPenn State Classes. Upon information and belief, Progress entered into contracts with DDCA and Affiliates to provide secure file transfer services to them, servers, and/or related equipment and services that included access to and use of the MOVEit software, data security practices, procedures, and protocols related to the MOVEit software sufficient to safeguard the Delta Dental Bellwether Plaintiffs and DDCA, DDIC, DDNY, and DDPenn Class Members' Private Information that was entrusted to DDCA and Affiliates.

2724. Upon information and belief, contracts between Progress and the DDCA and Affiliates were virtually identical and were made expressly for the benefit of DDCA and Affiliates' customers, including Delta Dental Bellwether Plaintiffs and DDCA, DDIC, DDNY, and DDPenn Class Members, as it was their Private Information that Progress agreed to receive, store, utilize, transfer, and protect through their services, so that DDCA and Affiliates could provide them dental insurance services. Thus, the benefit of collection, use, and protection of the Private Information belonging to Delta Dental Bellwether Plaintiffs and DDCA, DDIC, DDNY, and DDPenn Class Members was the direct and primary objective of the contracting parties, and Delta Dental Bellwether Plaintiffs and DDCA, DDIC, DDNY, and DDPenn Class Members were direct and express beneficiaries of such contracts.

2725. DDCA and Affiliates knew or should have known that if they were to breach these contracts, Delta Dental Bellwether Plaintiffs and DDCA, DDIC, DDNY, and DDPenn Class Members would be harmed.

2726. DDCA and Affiliates breached their contracts by, among other things, failing to adequately secure Delta Dental Bellwether Plaintiffs' and DDCA, DDIC, DDNY, and DDPenn Class Members' Private Information, and, as a result, Delta Dental Bellwether Plaintiffs and DDCA, DDIC, DDNY, and DDPenn Class Members were harmed.

2727. As a direct and proximate result of DDCA and Affiliates' breach, Delta Dental Bellwether Plaintiffs and DDCA, DDIC, DDNY, and DDPenn Class Members are at a current and ongoing risk of identity theft, and have already sustained incidental and consequential damages including: (i) financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out-of-pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) diminution of value of their Private Information; (vii) future costs of identity theft monitoring; and (viii) the continued risk to their Private Information, which remains in DDCA and Affiliates' control, and which is subject to further breaches, so long as DDCA and Affiliates fail to undertake appropriate and adequate measures to protect Delta Dental Bellwether Plaintiffs' and DDCA, DDIC, DDNY, and DDPenn Class Members' Private Information.

2728. Delta Dental Bellwether Plaintiffs and DDCA, DDIC, DDNY, and DDPenn Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

DELTA DENTAL BELLWETHER ELEVENTH CLAIM FOR RELIEF
Breach Of Fiduciary Duty
(On Behalf of the Delta Dental Nationwide Classes, or in the alternative, the Delta Dental Bellwether State Classes)

2729. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2730. Delta Dental Bellwether Plaintiffs bring this claim against DDA on behalf of the DDA Nationwide Class, or, in the alternative, the DDA State Classes. In addition, the Delta Dental

Bellwether Plaintiffs bring this claim against DDCA on behalf of the DDCA Nationwide Class, or, in the alternative, the DDCA State Classes. The DDIC Bellwether Plaintiffs bring this claim against DDIC on behalf of the DDIC Nationwide Class or, in the alternative, the DDIC State Classes. Plaintiff Michelle Gonsalves brings this claim against DDNY on behalf of the DDNY Nationwide Class or, in the alternative, the DDNY NY Class. The DDPenn Bellwether Plaintiffs bring this claim against DDPenn on behalf of the DDPenn Nationwide Class, or, in the alternative, the DDPenn State Classes. In light of the special relationship between Delta Dental Bellwether Defendants and Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members, Delta Dental Bellwether Defendants became fiduciaries by undertaking a guardianship of the Private Information to act primarily for the benefits of Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members. This duty included their obligations to (1) safeguard Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information, (2) provide timely notification to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members of a Data Breach and disclosure, and (3) maintain complete and accurate records of what information (and where) Delta Dental Bellwether Defendants do store.

2731. Delta Dental Bellwether Defendants had a fiduciary duty to act for the benefit of Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members upon matters within the scope of their relationship with their customers, in particular, to keep their Private Information secure, protected, and confidential.

2732. In order to provide Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members dental insurance services, Delta Dental Bellwether Defendants required that they provide their Private Information. This information was required to receive dental insurance through any of DDA's 39 member companies, which transferred Delta Dental Bellwether

Plaintiffs' and Delta Dental Bellwether Class Members' Private Information to DDA after it was provided.

2733. Delta Dental Bellwether Defendants knowingly undertook the responsibility and duties related to the possession of Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information.

2734. Delta Dental Bellwether Defendants breached their fiduciary duties owed to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members by failing to properly protect Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information by ensuring the integrity of the systems where they collected, stored, and transmitted the data. Delta Dental Bellwether Defendants further breached their fiduciary duties owed to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members by failing to timely detect the Data Breach and notify and/or warn Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members of the Data Breach.

2735. As a direct and proximate result of Delta Dental Bellwether Defendants' breach of their fiduciary duty, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, publication, release, theft, use, and/or viewing of their Private Information, and corresponding loss of value in their Private Information, and loss of value in their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to

prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in DDCA and Affiliates' possession and is subject to further unauthorized disclosures so long as Delta Dental Bellwether Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their or their business associates' continued possession, including to ensure that they retain vendors who adequately protect Private Information; (vi) future costs in terms of time, effort, and money that will be expended be expended to prevent, detect, and repair the impact of the Private Information compromised as a direct and traceable result of the Data Breach for the remainder of the lives of Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members; (vii) the diminished value of Delta Dental Bellwether Defendants' services they received; and (viii) nominal damages.

2736. As a direct and proximate result of Delta Dental Bellwether Defendants' breach of their fiduciary duty, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses. Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members seek actual and nominal damages for these harms.

DELTA DENTAL BELLWETHER TWELFTH CLAIM FOR RELIEF
Declaratory Judgment Act
28 U.S.C. §§ 2201, *et seq.*
(On Behalf of the Delta Dental Nationwide Classes, or in the alternative, the Delta Dental Bellwether State Classes)

2737. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2738. Delta Dental Bellwether Plaintiffs bring this claim against DDA on behalf of the DDA Nationwide Class, or, in the alternative, the DDA State Classes. In addition, the Delta Dental

Bellwether Plaintiffs bring this claim against DDCA on behalf of the DDCA Nationwide Class, or, in the alternative, the DDCA State Classes. The DDIC Bellwether Plaintiffs bring this claim against DDIC on behalf of the DDIC Nationwide Class or, in the alternative, the DDIC State Classes. Plaintiff Michelle Gonsalves brings this claim against DDNY on behalf of the DDNY Nationwide Class or, in the alternative, the DDNY NY Class. The DDPenn Bellwether Plaintiffs bring this claim against DDPenn on behalf of the DDPenn Nationwide Class, or, in the alternative, the DDPenn State Classes. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

2739. Delta Dental Bellwether Defendants owed a duty of care to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members, which required them to adequately monitor and safeguard Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information.

2740. Delta Dental Bellwether Defendants still possess the Private Information belonging to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members.

2741. Upon information and belief, Delta Dental Bellwether Defendants' data security measures remain inadequate.

2742. Furthermore, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

2743. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Delta Dental Bellwether Defendants owe a legal duty to secure Delta Dental Bellwether Plaintiffs' and Delta Dental Bellwether Class Members' Private Information under the common law, HIPAA, the FTCA, the California Medical Information Act, and other state and federal laws and regulations, as set forth herein;

b. Delta Dental Bellwether Defendants' existing data monitoring measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect individuals' Private Information; and

c. Delta Dental Bellwether Defendants continue to breach this legal duty by failing to employ reasonable measures to secure Delta Dental Bellwether Plaintiffs' and Class Members' Private Information.

2744. This Court should also issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with legal and industry standards to protect members' Private Information, as described in the Prayer for Relief.

2745. If an injunction is not issued, Delta Dental Bellwether Plaintiffs and Class Members will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach of the DDCA network environment compromised in this Data Breach or systems of Delta Dental Bellwether otherwise. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable and they will be forced to bring multiple lawsuits to rectify the same conduct.

2746. The hardship to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members if an injunction is not issued exceeds the hardship to Delta Dental Bellwether Defendants if an injunction is issued. Among other things, if another massive data breach occurs , Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members will likely be

subjected to substantial identity theft and other damage. On the other hand, the cost to Delta Dental Bellwether Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Delta Dental Bellwether Defendants have a pre-existing legal obligation to employ such measures.

2747. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach of Delta Dental Bellwether Defendants' systems and network, thus preventing future injury to Delta Dental Bellwether Plaintiffs and Delta Dental Bellwether Class Members whose Private Information would be further compromised.

DELTA DENTAL BELLWETHER THIRTEENTH CLAIM FOR RELIEF
California Customer Records Act ("CCRA")
Cal. Civ. Code §§ 1798.80, *et seq.*
(On Behalf of the DDCA Nationwide Class or, alternatively, the DDCA State Classes, the DDA Nationwide Class or, alternatively, the DDA State Classes, and the DDCA and DDA California Classes)

2748. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2749. Delta Dental Bellwether Plaintiffs bring this claim against DDCA on behalf of the DDCA Nationwide Class or, alternatively, the DDCA State Classes, and against DDA on behalf of the DDA Nationwide Class or, alternatively, the DDA State Classes. Plaintiffs Duarte and Moralez also bring this claim against DDCA on behalf of the DDCA California Class and DDA on behalf of the DDA California Class.

2750. "[T]o ensure that personal information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains personal information about a California resident shall implement and

maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

2751. The Private Information of Delta Dental Bellwether Plaintiffs and members of the DDCA Nationwide Class, DDCA State Classes, DDA Nationwide Class, DDA State Classes, DDCA California Class, and DDA California Class (collectively, "Delta Dental CA Statutory Classes") constitutes "personal information" under § 1798.80(e), hereafter "Private Information."

2752. DDCA is a business that owns, maintains, and licenses personal information within the meaning of Cal. Civ. Code §§ 1798.80(a) and 1798.81.5(b), about Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members.

2753. As alleged herein, DDCA failed to implement and maintain reasonable security procedures and practices appropriate to protect the unauthorized access, use and disclosure of Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' Private Information, in violation of § 1798.81.5(b).

2754. Businesses that own or license computerized data that includes Private Information are required to notify California residents when their Private Information has been acquired, "or is reasonably believed to have been[] acquired by an unauthorized person" in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82(a). Among other requirements, the security breach notification must include "the types of personal information that were or are reasonably believed to have been the subject of the breach" pursuant to the model security breach form provided in Cal. Civ. Code § 1798.82(d).

2755. DDCA is a business that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.80 and was thus subject to the disclosure requirements of Cal. Civ. Code § 1798.82.

2756. Because DDCA reasonably believed that Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' Private Information was acquired by unauthorized persons during the Data Breach, DDCA had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

2757. DDCA failed to fully disclose material information about the Data Breach in a timely and accurate manner, DDCA violated Cal. Civ. Code § 1798.82.

2758. By waiting over five and a half months—at minimum—to notify Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members that DDCA's and DDA's customer data had been compromised, Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members were prevented from taking appropriate, reasonable precautions to mitigate harms caused by the Data Breach.

2759. As a direct and proximate result of DDCA's and DDA's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members suffered damages, as described above.

2760. Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

DELTA DENTAL BELLWETHER FOURTEENTH CLAIM FOR RELIEF
California Confidentiality Of Medical Information Act ("CMIA")
Cal. Civ. Code §§ 56, *et seq.*
(On Behalf of the DDCA Nationwide Class or, alternatively, the DDCA State Classes, the DDA Nationwide Class or, alternatively, the DDA State Classes, and the DDCA and DDA California Classes)

2761. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2762. Delta Dental Bellwether Plaintiffs bring this claim against DDCA on behalf of the DDCA Nationwide Class or, alternatively, the DDCA State Classes, and against DDA on behalf of the DDA Nationwide Class or, alternatively, the DDA State Classes. Plaintiffs Duarte and Moralez also bring this claim against DDCA on behalf of the DDCA California Class and DDA on behalf of the DDA California Class.

2763. California's Confidentiality of Medical Information Act was enacted to protect, among other things, the release of confidential medical information without proper authorization. To that end, the CMIA prohibits entities from negligently disclosing or releasing any person's confidential medical information. See Cal. Civ. Code § 56.36.

2764. As described throughout this Complaint, Defendants negligently disclosed and released California Delta Dental Bellwether Plaintiffs' and California Subclass Members' Private Information inasmuch as they did not implement adequate security protocols to prevent unauthorized access to Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' Private Information, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially available measures to mitigate the risks of any data breach or otherwise comply with HIPAA data security requirements, including

ensuring that third-party vendors have implemented adequately safe, secure, and legally compliant policies and practices.

2765. As a direct and proximate result of DDCA's and DDA's conduct, the Data Breach occurred and DDCA and DDA negligently disclosed and released Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' Private Information to cybercriminals.

2766. As a direct and proximate result of this unauthorized disclosure, Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' unencrypted Private Information was viewed by unauthorized persons.

2767. Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members have suffered from the diminution of value of their Private Information, opportunity costs, among other economic injuries.

2768. Accordingly, Delta Dental Bellwether Plaintiffs, on behalf of themselves and the Delta Dental CA Statutory Classes , seek to recover actual, nominal (including $1,000 nominal damages per disclosure under § 56.36(b)), and statutory damages (including under § 56.36(c)) where applicable, together with reasonable attorneys' fees and costs.

DELTA DENTAL BELLWETHER FIFTEENTH CLAIM FOR RELIEF
California Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(On Behalf of the DDCA Nationwide Class or, alternatively, the DDCA State Classes, the DDA Nationwide Class or, alternatively, the DDA State Classes, and the DDCA and DDA California Classes)

2769. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2770. Delta Dental Bellwether Plaintiffs bring this claim against DDCA on behalf of the DDCA Nationwide Class or, alternatively, the DDCA State Classes, and against DDA on behalf

of the DDA Nationwide Class or, alternatively, the DDA State Classes. Plaintiffs Duarte and Moralez also bring this claim against DDCA on behalf of the DDCA California Class and DDA on behalf of the DDA California Class.

2771. The servers affected by the Data Breach were controlled and managed by DDCA and held all Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' Private Information.

2772. DDCA and DDA each satisfy the definition of a "person" as defined by Cal. Bus. & Prof. Code § 17201.

2773. Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members each satisfy the definition of a "person" as defined by Cal. Bus. & Prof. Code § 17201.

2774. Cal. Bus. & Prof. Code § 17204 provides that "a person who has suffered injury in fact and has lost money or property as a result of the unfair competition" may file suit.

2775. DDCA and DDA violated Cal. Bus. & Prof. Code § 17200 *et seq*. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

2776. DDCA's and DDA's "unfair" acts and practices include:

a. Failure to implement and maintain reasonable security measures to protect Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach, Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' Private Information being compromised, and subsequent harms caused to Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members.

b. Failure to identify foreseeable security risks, including in their third-party vendor, Progress, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

c. Failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use

appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45; California's Consumer Records Act, Cal. Civ. Code § 1798.81.5;; HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902;

d. Failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of DDCA's and DDA's inadequate security practices and policies, consumers could not have reasonably avoided the harms that DDCA and DDA caused; and

e. With respect to DDCA, engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82 disclosure requirements.

2777. DDCA and DDA engaged in "unlawful" business practices by violating multiple laws, including California's Customer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification); the FTC Act, 15 U.S.C. § 45; California common law; the California Constitution's Right to Privacy (Art I, § 1); HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902.

2778. DDCA and DDA engaged in "unlawful" business practices by violating multiple laws, including the FTC Act, 15 U.S.C. § 45; California common law; the California Constitution's Right to Privacy (Art I, § 1); HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902.

2779. DDCA's and DDA's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' Private Information, which was a direct and proximate cause of the Data Breach, Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' Private Information being compromised, and subsequent harms caused to Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach, unauthorized disclosure of Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' Private Information, and subsequent harms;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' Private Information, including duties imposed by the FTC Act, 15 U. S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 et seq., HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902, which was a direct and proximate cause of the Data Breach, Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' Private Information being compromised, and subsequent harms caused to Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members;

d. Misrepresenting that they would protect the privacy and confidentiality of Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.; HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq.; HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902.

2780. DDCA's and DDA's unfair and unlawful acts, e.g., failing to implement adequate security practices, harmed Delta Dental Bellwether Plaintiffs and the Delta Dental CA Statutory Class.

2781. DDCA's and DDA's representations and omissions were material because they were likely to deceive reasonable consumers, including the Delta Dental CA Statutory Class

Members, about the adequacy of DDCA's and DDA's respective data security policies and practices and ability to protect the confidentiality of consumers' Private Information.

2782. Had DDCA and DDA disclosed to consumers that they were not complying with industry standards or regulations or that their data systems were not secure and, thus, were vulnerable to attack, they would have been unable to continue in business and they would have been forced to adopt reasonable data security measures and comply with the law.

2783. Accordingly, Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members acted reasonably in relying on DDCA's and DDA's misrepresentations and omissions, the truth of which they could not have discovered.

2784. DDCA and DDA were entrusted, either directly or indirectly, with sensitive and valuable Private Information regarding millions of consumers, including that of Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members. DDCA and DDA accepted the critical responsibility of protecting the data but kept the inadequate state of their security controls secret from the public.

2785. As a direct and proximate result of DDCA's and DDA's unfair, unlawful, and/or fraudulent acts and practices, Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for DDCA's and DDA's dental insurance; loss of the value of access to their Private Information; and the value of identity and credit protection and repair services made necessary by the Data Breach.

2786. Defendants' violations were, and are, willful, deceptive, unfair, and unconscionable.

2787. Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members have lost money and property as a result of DDCA's and DDA's conduct in violation of the UCL, as stated herein and above.

2788. By deceptively, unfairly, and unlawfully storing, collecting, and disclosing their Private Information, DDCA and DDA have taken money or property from Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members. DDCA and DDA acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' rights.

2789. DDCA and DDA were aware that the healthcare industry was a frequent target of sophisticated cyberattacks due to the high market value of Private Information and on notice of the risks posed to consumers' Private Information that they collected, stored, used, and transferred.

2790. DDCA and DDA were on notice that their security and privacy policies and practices were wholly inadequate, including that of ensuring their vendors were compliant with industry standards and regulations, because of previous data breaches against Delta Dental Companies within the DDA national network that implement the same data security policies and practices.

2791. Delta Dental Bellwether Plaintiffs and Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from DDCA's and DDA's unfair, unlawful, and fraudulent business practices or use of their Private Information;

declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

DELTA DENTAL BELLWETHER SIXTEENTH CLAIM FOR RELIEF
California Constitution's Right To Privacy
Cal. Const., Art. I, § I
(On Behalf of the DDCA Nationwide Class or, alternatively, the DDCA State Classes, the DDA Nationwide Class or, alternatively, the DDA State Classes, and the DDCA and DDA California Classes)

2792. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2793. Delta Dental Bellwether Plaintiffs bring this claim against DDCA on behalf of the DDCA Nationwide Class or, alternatively, the DDCA State Classes, and against DDA on behalf of the DDA Nationwide Class or, alternatively, the DDA State Classes. Plaintiffs Duarte and Moralez also bring this claim against DDCA on behalf of the DDCA California Class and DDA on behalf of the DDA California Class.

2794. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

2795. The right to privacy in California's Constitution creates a private right of action against private and government entities.

2796. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

2797. DDCA and DDA violated Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' constitutional right to privacy by collecting, storing, and disclosing, or preventing from unauthorized disclosure, their personal identifying information and protected health information, which includes in which they had a legally protected privacy interest, and for which they had a reasonable expectation of privacy. Disclosure of their Private Information was highly offensive given the highly sensitive nature of the data. Disclosure of their private medical information in particular could cause humiliation to Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members. Accordingly, disclosure of Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' Private Information is an egregious violation of social norms.

2798. DDCA and DDA intruded upon Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential Private Information.

2799. Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members had a reasonable expectation of privacy in that: (i) their invasion of privacy occurred as a result of DDCA's and DDA's lax and inadequate security practices with respect to securely collecting, storing, and using data, as well as preventing the unauthorized disclosure of their Private Information; (ii) Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members did not consent or otherwise authorize DDCA and DDA to disclose their Private Information to parties responsible for the cyberattack; and (iii) Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members could not reasonably expect DDCA and DDA would commit acts in violation of laws protecting their privacy.

2800. As a result of DDCA's and DDA's actions, Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members have been damaged as a direct and proximate result of DDCA's and DDA's invasion of their privacy and are entitled to just compensation.

2801. Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members suffered actual and concrete injury as a result of DDCA's and DDA's violations of their privacy interests. Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members are entitled to appropriate relief, including damages to compensate them for the harms to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by DDCA's and DDA's invasions.

2802. Delta Dental Bellwether Plaintiffs and Delta Dental CA Statutory Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate them for the harm to their privacy interests as well as disgorgement of profits made by DDCA and DDA as a result of their intrusions upon Delta Dental Bellwether Plaintiffs' and Delta Dental CA Statutory Class Members' privacy.

DELTA DENTAL BELLWETHER SEVENTEENTH CLAIM FOR RELIEF
California Consumer Legal Remedies Act
Cal. Civ. Code §§ 1750, *et seq.*
(On Behalf of the DDCA Nationwide Class or, alternatively, the DDCA State Classes, the DDA Nationwide Class or, alternatively, the DDA State Classes, and the DDCA and DDA California Classes)

2803. The Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One and Chapter Two.

2804. Delta Dental Bellwether Plaintiffs bring this claim against DDCA on behalf of the DDCA Nationwide Class or, alternatively, the DDCA State Classes, and against DDA on behalf

of the DDA Nationwide Class or, alternatively, the DDA State Classes. Plaintiffs Duarte and Moralez also bring this claim against DDCA on behalf of the DDCA California Class and DDA on behalf of the DDA California Class.

2805. At all relevant times, the Delta Dental Bellwether Plaintiffs and members of the DDCA California Class and DDA California Class were "consumers" as under the terms of the CLRA as individuals seeking or acquiring, by purchase or lease, goods or services for personal, family, or household purposes.

2806. At all relevant times DDCA's and DDA's actions and conduct resulted in transactions for the sale or lease of goods or services to consumers under the terms of the Consumer Legal Remedies Act ("CLRA").

2807. By the acts described above, DDCA and DDA violated California Civil Code section 1770(a)(5), by the use of untrue or misleading statements and omissions and representing that their services had characteristics or benefits that it knew to be untrue, namely that DDCA and DDA had adequate data privacy practices and protections to safeguard Delta Dental Bellwether Plaintiffs' Private Information and the Private Information of members of the DDCA California Class and DDA California Class.

2808. By the acts described above, DDCA and DDA violated California Civil Code section 1770(a)(14), by representing to its clients and the public at large that they employed the highest level of data security and would protect and safeguard Private Information from unauthorized, knowing and intending that these representations would reach Delta Dental Bellwether Plaintiffs and members of the DDCA California Class and DDA California Class, when in fact DDCA and DDA knew such benefits were not conferred.

2809. DDCA and DDA knew, or should have known, that their representations and advertisements about the nature of their data security and abilities to securely store and transfer Private Information were false or misleading and were likely to deceive a reasonable consumer. No reasonable consumer would use DDCA's and DDA's services if they knew that they were not taking reasonable measures to safeguard their Private Information.

2810. As a direct and proximate result of DDCA's and DDA's violations of California Civil Code § 1770, Delta Dental Bellwether Plaintiffs and members of the DDCA California Class and DDA California Class have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information, including, but not limited to, the diminishment of their present and future property interest in their Private Information and the deprivation of the exclusive use of their Private Information.

2811. Pursuant to California Civil Code § 1782(d), Delta Dental Bellwether Plaintiffs sent letters to DDCA and DDA on December 6, 2024, notifying them of their CLRA violations and providing them with the opportunity to correct their business practices. If DDCA and DDA do not hereafter correct their business practices, Delta Dental Bellwether Plaintiffs will amend (or seek leave to amend) this Bellwether Consolidated Class Action Complaint to add claims for monetary relief, including restitution, actual, and punitive damages under the CLRA.

2812. Delta Dental Bellwether Plaintiffs and members of the DDCA California Class and DDA California Class seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

DELTA DENTAL BELLWETHER EIGHTEENTH CLAIM FOR RELIEF
CONNECTICUT UNFAIR TRADE PRACTICES ACT ("CUTPA")
Conn. Gen. Stat. § 42-110B
(On Behalf of the DDCA Connecticut Class; the DDA Connecticut Class, and the DDIC Connecticut Class)

2813. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2814. Plaintiff Boginski brings this claim against DDA on behalf of the DDA Connecticut Class. In addition, Plaintiff Boginski brings this claim against DDCA on behalf of the DDCA Connecticut Class. Plaintiff Boginski also brings this claim against DDIC on behalf of the DDIC Connecticut Class.

2815. DDA, DDCA, DDIC, Plaintiff Boginski, DDA Connecticut Class Members, DDCA Connecticut Class Members, and DDIC Connecticut Class Members are "persons" within the meaning of Conn. Gen. Stat. § 42- 110a(3).

2816. The Connecticut Unfair Trade Practices provides: "No person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." Conn. Gen. Stat. § 42-110b(a).

2817. DDIC, DDCA, and DDA advertised, offered, sold, or distributed services in Connecticut and engaged in "trade" or "commerce" directly or indirectly affecting persons in Connecticut. Conn. Gen. Stat. § 42-110a(4).

2818. CUTPA provides that "[a]ny person who suffers an ascertainable loss of money or property, real or personal, as a result of the use or employment of a method, act or practice

prohibited by section 42-110b, may bring an action . . . to recover actual damages." Conn. Gen. Stat. § 42-110g(a).

2819. Plaintiff Boginski, DDA Connecticut Class Members, DDCA Connecticut Class Members, and DDIC Connecticut Class Members have a private right of action under Conn. Gen. Stat. § 42-110g(a).

2820. DDA, DDCA, and DDIC engaged in unfair or deceptive acts or practices in violation of Conn. Gen. Stat. § 42-110b(a) by, among other things:

a. Failing to implement and maintain reasonable security measures to protect Plaintiff Boginski, DDA Connecticut Class Members, DDCA Connecticut Class Members, and DDIC Connecticut Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach, Plaintiff Boginski, DDA Connecticut Class Members, DDCA Connecticut Class Members, and DDIC Connecticut Class Members' ' Private Information being compromised, and subsequent harms caused to Plaintiff Boginski, DDA Connecticut Class Members, DDCA Connecticut Class Members, and DDIC Connecticut Class Members;

b. Failing to identify foreseeable security risks, remediate identified security risks, and sufficiently improve security following previous cybersecurity incidents, as alleged herein. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff Boginski, DDA Connecticut Class Members, DDCA Connecticut Class Members, and DDIC Connecticut Class Members , whose Private Information has been compromised;

c. Misrepresenting, omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections they had in place to protect the Private Information of Plaintiff Boginski, DDA Connecticut Class Members, DDCA Connecticut Class Members, and DDIC Connecticut Class Members.

2821. DDA, DDCA, and DDIC's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45. Similarly, policies of the

importance of protecting individuals' PHI are reflected in HIPAA, 45 C.F.R. § 164; HITECH Act, 42 U.S.C. § 17902; and Conn. Gen. Stat. § 36A-701B.

2822. CUTPA provides that in its interpretation and application, the courts "shall be guided by interpretations given by the Federal Trade Commission and the federal courts to Section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. § 45(a)(1)), as from time to time amended." Conn. Gen. Stat. § 42-110b(b). As discussed, *supra*, the FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

2823. DDA, DDCA, and DDIC's failure to adequately safeguard Plaintiff Boginski, DDA Connecticut Class Members, DDCA Connecticut Class Members, and DDIC Connecticut Class Members' Private Information, constituting an unfair act under Gen. Stat. § 42-110b, was immoral, unethical, oppressive, and unscrupulous.

2824. DDA, DDCA, and DDIC were aware that the healthcare industry was a frequent target of sophisticated cyberattacks.

2825. DDA, DDCA, and DDIC knew or should have known that their data security policies and practices, including ensuring the integrity and security of their vendors' security practices, were deficient, inadequate, and did not satisfy industry or regulatory standards for the purposes of protecting consumers' Private Information, thus leaving their customers' Private Information vulnerable to attack.

2826. DDA, DDCA, and DDIC knew or should have known that its data security was insufficient to guard against those attacks, particularly, given the size of its database and the sensitivity of the Private Information therein.

2827. DDA, DDCA, and DDIC should have taken adequate measures to protect the data. DDA, DDCA, and DDIC's above-described conduct was negligent, knowing and willful, and/or wanton and reckless.

2828. Additionally, DDA, DDCA, and DDIC's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of their data security policies and practices and ability to protect the confidentiality of consumers' Private Information and thus were immoral, unethical, oppressive, and unscrupulous.

2829. DDA, DDCA, and DDIC's acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

2830. As a direct and proximate result of DDA, DDCA, and DDIC's deceptive acts and practices, Plaintiff Boginski, DDA Connecticut Class Members, DDCA Connecticut Class Members, and DDIC Connecticut Class Members suffered ascertainable losses, including the loss of their legally protected interest in the confidentiality and privacy of their Private Information, diminution in value of their Private Information, loss of time and opportunity costs, among others alleged herein.

2831. Additionally, as alleged, *infra*, DDA, DDCA, and DDIC's actions in violation of the CUTPA include, but are not limited to their failure to disclose the Data Breach in a timely and accurate manner as required by C.G.S.A. § 36a-701b(b) and (c).

2832. Specifically, DDA, DDCA, and DDIC unreasonably delayed issuing their first public notice to Plaintiff Boginski, DDA Connecticut Class Members, DDCA Connecticut Class Members, and DDIC Connecticut Class Members by issuing it over five months after allegedly

discovering the Data Breach that affected their company data, while also failing to accurately disclose information accurately, by vaguely referring to the incident in the delayed notice.

2833. DDA, DDCA, and DDIC's failure to disclose the Data Breach in a timely and accurate manner was misleading to Plaintiff Boginski, DDA Connecticut Class Members, DDCA Connecticut Class Members, and DDIC Connecticut Class Members as they reasonably believed their Private Information and other private and confidential information was secured by DDA, DDCA, and DDIC due to the sensitive nature of the data and special relationship they held, and promises of data security and privacy contained in multiple privacy policies and documents, among other reasons.

2834. DDA, DDCA, and DDIC failure to disclose was material since it affected Plaintiff Boginski, DDA Connecticut Class Members, DDCA Connecticut Class Members, and DDIC Connecticut Class Members' decisions, including but not limited to:

a. whether to continue to provide Private Information or other private and confidential information to DDA, DDCA, and DDIC;

b. whether to pay for services to attempt to secure Private Information compromised by the data breach;

c. whether to seek the advice of counsel and/or seek legal representation; and

d. whether to continue to use DDA, DDCA, and DDIC's services.

2835. DDA, DDCA, and DDIC's failure to disclose in a timely and accurate manner was immoral, unethical, oppressive, or unscrupulous since it deprived Plaintiff Boginski, DDA Connecticut Class Members, DDCA Connecticut Class Members, and DDIC Connecticut Class Members of important knowledge about their compromised Private Information and delayed any ability they had to try and secure their Private Information and other private and confidential information.

2836. Furthermore, DDA, DDCA, and DDIC's failure to disclose in a timely and accurate manner has caused substantial injury to Plaintiff Boginski, DDA Connecticut Class Members, DDCA Connecticut Class Members, and DDIC Connecticut Class Members since they were deprived of the knowledge their Private Information was compromised, and lost a substantial amount of time in which they could have acted to secure their Private Information in avoidance of the imminent, impending threats of identity theft, fraud, scams; loss of value of their stolen Private Information; illegal sales of the compromised Private Information on the black market; other misuses of their Private Information; monetary loss and economic harm; the need to pay for mitigation expenses and spend time spent monitoring credit; identity theft insurance costs; credit freezes/unfreezes, time spent initiating fraud alerts and contacting third parties; decreased credit scores; lost work time; mental anguish; and other injuries due to the Data Breach.

2837. DDA, DDCA, and DDIC's failure to disclose the Data Breach in a timely and accurate fashion as described above constitutes an unfair or deceptive act or practice in violation of CUTPA, C.G.S.A. § 42-110b.

2838. As a result of DDA, DDCA, and DDIC's failure to disclose the Data Breach in a timely and accurate fashion, Plaintiff Boginski, DDA Connecticut Class Members, DDCA Connecticut Class Members, and DDIC Connecticut Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages including but not limited to fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent and impending threat of fraud and identity theft, loss of value of their Private Information; overpayment for DDCA and Affiliates' dental insurance; loss of the value of access to their Private

Information; and the value of identity and credit protection and repair services made necessary by the Data Breach.

2839. Plaintiff Boginski, DDA Connecticut Class Members, DDCA Connecticut Class Members, and DDIC Connecticut Class Members seek relief under Conn. Gen. Stat. § 42-110g, including actual damages, punitive damages, injunctive relief, and attorneys' fees, expenses, and costs.

DELTA DENTAL BELLWETHER NINETEENTH CLAIM FOR RELIEF
GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT ("GUDTPA")
Ga. Code Ann. §§ 10-1-370, *et seq*.
(On Behalf of the DDA Georgia Class, the DDCA Georgia Class, the DDIC Georgia Class, and the DDPenn Georgia Class)

2840. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2841. Plaintiffs Doris Cadet and Taneisha Robertson bring this claim against DDA on behalf of the DDA Georgia Class. In addition, Plaintiffs Cadet and Robertson bring this claim against DDCA on behalf of the DDCA Georgia Class. Plaintiff Cadet brings this claim against DDIC on behalf of the DDIC Georgia Class. Plaintiff Roberton brings this claim against DDPenn on behalf of the DDPenn Georgia Class.

2842. DDIC, DDPenn, DDCA, DDA, Plaintiffs Cadet and Robertson, DDA Georgia Class Members, DDCA Georgia Class Members, DDIC Georgia Class Members, and DDPenn Georgia Class Members are "persons" within the meaning of Ga. Code Ann. § 10-1-371(5).

2843. DDA, DDCA, DDIC, and DDPenn engaged in deceptive trade practices in the conduct of their businesses, in violation of Ga. Code Ann. § 10-1-372(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with the intent not to sell them as advertised;

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

2844. DDA, DDCA, DDIC, and DDPenn's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs Cadet and Robertson, DDA Georgia Class Members, DDCA Georgia Class Members, DDIC Georgia Class Members, and DDPenn Georgia Class Members' Private Information, which was a direct and proximate cause of the Data Breach, their Private Information being compromised in the Data Breach and subsequent harms;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach, their Private Information being compromised in the Data Breach and subsequent harms;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy Plaintiffs Cadet and Robertson, DDA Georgia Class Members, DDCA Georgia Class Members, DDIC Georgia Class Members, and DDPenn Georgia Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902, which was a direct and proximate cause of the Data Breach, their Private Information being compromised in the Data Breach and subsequent harms;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs Cadet and Robertson, DDA Georgia Class Members, DDCA Georgia Class Members, DDIC Georgia Class Members, and DDPenn Georgia Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Cadet and Robertson, DDA Georgia Class Members, DDCA Georgia Class Members, DDIC Georgia Class Members, and DDPenn Georgia Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; and HIPAA, 45 C.F.R. § 164;

f. Omitting, suppressing, and concealing the material fact that they did not properly secure Plaintiffs Cadet and Robertson, DDA Georgia Class

Members, DDCA Georgia Class Members, DDIC Georgia Class Members, and DDPenn Georgia Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Cadet and Robertson, DDA Georgia Class Members, DDCA Georgia Class Members, DDIC Georgia Class Members, and DDPenn Georgia Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902.

2845. DDA, DDCA, DDIC, and DDPenn's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of their data security policies and practices and ability to protect the confidentiality of consumers' Private Information.

2846. In the course of their business, DDA, DDCA, DDIC, and DDPenn engaged in activities with a tendency or capacity to deceive.

2847. DDA, DDCA, DDIC, and DDPenn acted intentionally, knowingly, and maliciously to violate Georgia's Uniform Deceptive Trade Practices Act, and recklessly disregarded the rights of Plaintiffs Cadet and Robertson, DDA Georgia Class Members, DDCA Georgia Class Members, DDIC Georgia Class Members, and DDPenn Georgia Class Members. The various breaches of Delta Dental Companies within DDA's network put DDA, DDCA, DDIC, and DDPenn on notice that their security and privacy protections were inadequate.

2848. Had DDA, DDCA, DDIC, and DDPenn disclosed to consumers that they were not complying with industry standards or regulations or that their data systems were not secure and, thus, were vulnerable to attack, they would have been unable to continue in business and they would have been forced to adopt reasonable data security measures and comply with the law.

2849. Instead, DDA, DDCA, DDIC, and DDPenn were entrusted, either directly or indirectly, with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs Cadet and Robertson, DDA Georgia Class Members, DDCA Georgia Class

Members, DDIC Georgia Class Members, and DDPenn Georgia Class Members. DDA, DDCA, DDIC, and DDPenn accepted the critical responsibility of protecting the data but kept the inadequate state of their security controls secret from the public. Accordingly Plaintiffs Cadet and Robertson, DDA Georgia Class Members, DDCA Georgia Class Members, DDIC Georgia Class Members, and DDPenn Georgia Class Members acted reasonably in relying on DDA, DDCA, DDIC, and DDPenn's misrepresentations and omissions, the truth of which they could not have discovered.

2850. As a direct and proximate result of DDA, DDCA, DDIC, and DDPenn's unfair, unlawful, and fraudulent acts and practices, Plaintiffs Cadet and Robertson, DDA Georgia Class Members, DDCA Georgia Class Members, DDIC Georgia Class Members, and DDPenn Georgia Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for DDCA and Affiliates' dental insurance; loss of the value of access to their Private Information; diminution of value of Private Information; value of identity and credit protection and repair services made necessary by the Data Breach; and they face ongoing risks of future harms insofar as DDA, DDCA, DDIC, and DDPenn have yet to implement the necessary policies, practices, and measures to adequately safeguard their Private Information in compliance with laws and industry standards.

2851. Plaintiffs Cadet and Robertson, DDA Georgia Class Members, DDCA Georgia Class Members, DDIC Georgia Class Members, and DDPenn Georgia Class Members seek all relief allowed by law, including injunctive relief, which is necessary to prospectively protect

against future data breaches, and reasonable attorneys' fees and costs, under Ga. Code Ann. § 10-1-373.

DELTA DENTAL BELLWETHER TWENTIETH CLAIM FOR RELIEF
Violations of Illinois Personal Information Protection Act ("PIPA")
815 ILCS 530/10(a)
(Brought on behalf of the DDA Nationwide Class, or, in the alternative, the DDA State Classes)

2852. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2853. Delta Dental Bellwether Plaintiffs bring this claim against DDA on behalf of the DDA Nationwide Class, or, in the alternative, the DDA State Classes.

2854. Section 10(b) of PIPA states, in pertinent part:

> [a]ny data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

815 ILCS 530/10(b).

2855. DDA conducts business in Illinois. DDA is an Illinois 501(c)(6) not-for-profit national network of Delta Dental Companies, headquartered in Oak Brook, Illinois. Its business within the state consists of the marketing, sale, delivery, maintenance, and administration of thousands of dental plans.

2856. DDA is a "data collector[s]" as defined by the statute because each is a company that "handles, collects, disseminates, or otherwise deals with nonpublic personal information." 815 ILCS 530/5.

2857. Delta Dental Bellwether Plaintiffs' and DDA Class Members' claims are based on their statuses as "owner[s]" of their PII.

2858. DDA failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

2859. Section 45 of PIPA requires entities who maintain or store "personal information concerning an Illinois resident" to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure."

2860. DDA's conduct violated PIPA because they voluntarily undertook the act of maintaining and storing Delta Dental Bellwether Plaintiffs' and DDA Class Members' PII, but failed to implement safety and security procedures and practices sufficient enough to protect the PII from the Data Breach that they should have anticipated.

2861. DDA should have known and anticipated that data breaches were on the rise and that software companies were lucrative or likely targets of cyber criminals looking to steal PII. Therefore, DDA should have implemented and maintained procedures and practices appropriate to the nature and scope of information compromised in the Data Breach.

2862. As a result of DDA's violation of PIPA, Delta Dental Bellwether Plaintiffs and DDA Class Members incurred economic damages, including expenses associated with necessary credit monitoring.

DELTA DENTAL BELLWETHER TWENTY-FIRST CLAIM FOR RELIEF
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA")
815 ILCS 505/1, *et seq.*
(Brought on behalf of the DDA Nationwide Class, or, in the alternative, the DDA State Classes)

2863. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2864. Delta Dental Bellwether Plaintiffs bring this claim against DDA on behalf of the DDA Nationwide Class, or, in the alternative, the DDA State Classes.

2865. Section 2 of ICFA prohibits unfair or deceptive acts or practices and states, in relevant part, as follows:

2866. Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of such material fact, or the use or employment of any practice described in section 2 of the "Uniform Deceptive Trade Practices Act", approved August 5, 1965, in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby.

2867. DDA violated Section 2 of ICFA by engaging in unfair acts in the course of conduct involving trade or commerce when dealing with Delta Dental Bellwether Plaintiffs. Specifically, it was an unfair act and practice for DDA to represent to the public that they implemented commercially reasonable measures to protect Delta Dental Bellwether Plaintiffs' and DDA Class Members' PII when it knew or should have known that they failed to fulfill such representations, including by preventing and failing to timely detect the Data Breach.

2868. Despite representing to Delta Dental Bellwether Plaintiffs and DDA Class Members that they would implement commercially reasonable measures to protect their PII, DDA nonetheless failed to fulfill such representations.

2869. Delta Dental Bellwether Plaintiffs and the DDA Class Members have suffered injury in fact and actual damages, as alleged herein, as a result of DDA's unlawful conduct and violations of the ICFA and analogous state statutes.

2870. DDA's conduct offends public policy as it demonstrates a practice of unfair and deceptive business practices in failing to safeguard consumers' PII.

2871. An award of punitive damages is appropriate because DDA's conduct described above was outrageous, willful and wanton, showed a reckless disregard for the rights of Delta Dental Bellwether Plaintiffs and consumers, generally, and Delta Dental Bellwether Plaintiffs and DDA Class Members had no choice but to submit to Delta Dental's illegal conduct.

DELTA DENTAL BELLWETHER TWENTY-SECOND CLAIM FOR RELIEF
Violation of the Illinois Uniform Deceptive Trade Practices Act
815 Ill. Comp. Stat. §§ 510/2, *et seq.*
(Brought on behalf of the DDA Nationwide Class, or, in the alternative, the DDA State Classes)

2872. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2873. Delta Dental Bellwether Plaintiffs bring this claim against DDA on behalf of the DDA Nationwide Class, or, in the alternative, the DDA State Classes.

2874. DDA is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

2875. DDA engaged in deceptive trade practices in the conduct of their businesses, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including, but not limited to:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

2876. DDA's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Delta Dental Bellwether Plaintiffs' and DDA Class Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Delta Dental Bellwether Plaintiffs' and DDA Class Members' PII, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Delta Dental Bellwether Plaintiffs' and DDA Class Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Delta Dental Bellwether Plaintiffs' and DDA Class Members' PII;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Delta Dental Bellwether Plaintiffs' and DDA Class Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Delta Dental Bellwether Plaintiffs' and DDA Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

2877. DDA's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of their data security and ability to protect the confidentiality of consumers' PII.

2878. The above unfair and deceptive practices and acts by DDA were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Delta Dental Bellwether Plaintiffs and the DDA Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

2879. As a direct and proximate result of DDA's unfair, unlawful, and deceptive trade practices, Delta Dental Bellwether Plaintiffs and the DDA Class Members have suffered and will continue to suffer injury.

2880. Delta Dental Bellwether Plaintiffs and the DDA Class Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees and costs.

DELTA DENTAL BELLWETHER TWENTY-THIRD CLAIM FOR RELIEF
Massachusetts General Laws Chapter 93A
M.G.L. ch. 93A §§ 2 and 9
(On Behalf of Delta Dental Bellwether Nationwide Classes, or, in the alternative, the Delta Dental Bellwether State Classes)

2881. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2882. Delta Dental Bellwether Plaintiffs bring this claim against Delta Dental Bellwether Defendants on behalf of the Delta Dental Nationwide Classes or, alternatively, the Delta Dental State Classes.

2883. M.G.L. ch. 93A § 2 provides that "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." M.G.L. ch. 93A § 9 permits any consumer injured by a violation of M.G.L. ch. 93A § 2 to bring a civil action, including a class action, for damages and injunctive relief.

2884. Delta Dental Bellwether Plaintiffs allege Delta Dental Bellwether Defendants committed unfair business acts and/or practices in violation of M.G.L. ch. 93A §§ 2 and 9.

2885. Delta Dental Bellwether Defendants knew or should have known of the inherent risks in experiencing a data breach if they failed to maintain adequate systems and processes for keeping Delta Dental Bellwether Plaintiffs' and Delta Dental Class Members' Private Information safe and secure. Only Delta Dental Bellwether Defendants were in a position to ensure that their systems were sufficient to protect against harms to Delta Dental Bellwether Plaintiffs and the Delta Dental Class resulting from a data security incident such as the Data Breach; instead, they failed to implement such safeguards.

2886. Delta Dental Bellwether Defendants' own conduct also created a foreseeable risk of harm to Delta Dental Bellwether Plaintiffs and Delta Dental Class Members and their Private Information. Delta Dental Bellwether Defendants' misconduct included failing to adopt, implement, and maintain the systems, policies, and procedures necessary to prevent the Data Breach.

2887. Delta Dental Bellwether Defendants acknowledge their conduct created actual harm to Delta Dental Bellwether Plaintiffs and Delta Dental Class Members because Delta Dental Bellwether Defendants instructed them to monitor their accounts for fraudulent conduct and identity theft.

2888. Delta Dental Bellwether Defendants knew, or should have known, of the risks inherent in disclosing, collecting, storing, accessing, and transmitting Private Information and the importance of adequate security because of, *inter alia*, the prevalence of data breaches.

2889. Delta Dental Bellwether Defendants failed to adopt, implement, and maintain fair, reasonable, or adequate security measures to safeguard Delta Dental Bellwether Plaintiffs' and

Delta Dental Class Members' Private Information, failed to recognize in a timely manner the Data Breach, and failed to notify Delta Dental Bellwether Plaintiffs and Delta Dental Class Members in a timely manner that their Private Information was accessed in the Data Breach.

2890. These acts and practices are unfair in material respects, offend public policy, are immoral, unethical, oppressive and unscrupulous and violate 201 CMR 17.00 and M.G.L. ch. 93A § 2.

2891. As a direct and proximate result of Delta Dental Bellwether Defendants' unfair acts and practices, Delta Dental Bellwether Plaintiffs and Delta Dental Class Members have suffered injury and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their Private Information is used; (ii) the publication and/or fraudulent use of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from unemployment and/or tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Private Information, which remains in Delta Dental Bellwether Defendants' possession (and/or to which Delta Dental Bellwether Defendants continue to have access) and is subject to further unauthorized disclosures so long as Delta Dental Bellwether Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession; and, (viii) future costs in terms of time, effort and money that will

be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of disclosed Private Information.

2892. Neither Delta Dental Bellwether Plaintiffs nor the other Delta Dental Class Members contributed to the Data Breach.

2893. Delta Dental Bellwether Plaintiffs sent a demand for relief, in writing, to Delta Dental Bellwether Defendants on June 4, 2024, prior to filing this complaint. Multiple plaintiffs in consolidated actions have sent[729]—or alleged in their complaints that they would send[730]—similar demand letters as required by M.G.L. c. 93A § 9. Delta Dental Bellwether Plaintiffs have not received a written tender of settlement that is reasonable in relation to the injury actually suffered by Delta Dental Bellwether Plaintiffs and Delta Dental Class Members.

2894. Based on the foregoing, Delta Dental Bellwether Plaintiffs and Delta Dental Class Members are entitled to all remedies available pursuant to M.G.L ch. 93A, including, but not limited to, refunds, actual damages, or statutory damages in the amount of twenty-five dollars per

[729] *See, e.g.*, *Ghalem, et al. v. Progress Software Corp., et al.*, 23-cv-12300 (D. Mass.), at ECF No. 1, ¶ 213 ("A demand identifying the claimant and reasonably describing the unfair or deceptive act or practice relied upon and the injury suffered was mailed or delivered to Defendants at least thirty days prior to the filing of a pleading alleging this claim for relief").

[730] In all of the following cases (among others), plaintiffs indicated that they were going to send similar demand letters: *Allen, et al. v. Progress Software Corp*., 23-cv-11984 (D. Mass.); *Anastasio v. Progress Software Corp., et al*., 23-cv-11442 (D. Mass.); *Arden v. Progress Software Corp., et al*., 23-cv-12015 (D. Mass.); *Boaden v. Progress Software Corp., et al*., 23-cv-12192 (D. Mass.); *Brida v. Progress Software Corp., et al*., 23-cv-12202 (D. Mass.); *Casey v. Progress Software Corp., et al*., 23-cv-11864 (D. Mass.); *Constantine v. Progress Software Corp., et al*., 23-cv-12836 (D. Mass.); *Daniels v. Progress Software Corp., et al*., 23-cv-12010 (D. Mass.); *Doe v. Progress Software Corp., et al*., 23-cv-1933 (D. Md.); *Ghalem, et al. v. Progress Software Corp., et al*., 23-cv-12300 (D. Mass.); *Kennedy v. Progress Software Corp., et al*., 23-cv-12275 (D. Mass.); *Kurtz v. Progress Software Corp., et al*., 23-cv-12156 (D. Mass.); *McDaniel, et al. v. Progress Software Corp., et al*., 23-cv-11939 (D. Mass.); *Pilotti-Iulo v. Progress Software Corp., et al*., 23-cv-12157 (D. Mass.); *Pulignani v. Progress Software Corp., et al*. , 23-cv-1912 (D. Md.); *Siflinger, et al. v. Progress Software Corp., et al*., 23-cv-11782 (D. Mass.); *Tenner v. Progress Software Corp*., 23-cv-11412 (D. Mass.); *Truesdale v. Progress Software Corp., et al*., 23-cv-1913 (D. Md.).

violation, whichever is greater, double or treble damages, attorneys' fees and other reasonable costs.

2895. Pursuant to M.G.L. ch. 231, § 6B, Delta Dental Bellwether Plaintiffs and Delta Dental Class Members are further entitled to pre-judgment interest as a direct and proximate result of Progress's wrongful conduct. The amount of damages suffered as a result is a sum certain and capable of calculation, and Delta Dental Bellwether Plaintiffs and Delta Dental Class Members are entitled to interest in an amount according to proof.

DELTA DENTAL BELLWETHER TWENTY-FOURTH CLAIM FOR RELIEF
New York Deceptive Trade Practices Act ("GBL")
N.Y. Gen. Bus. Law. § 349
(On Behalf of the DDCA New York Class, DDA New York Class, and DDNY New York Class)

2896. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2897. Delta Dental Bellwether Plaintiffs Gonsalves and Kavanagh bring this claim against DDCA, DDA, and DDNY on behalf of the DDCA New York Class, DDA New York Class, and DDNY New York Class.

2898. DDCA, DDA, and DDNY engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs Gonsalves' and Kavanagh's Private Information and the Private Information of members of the DCA New York Class, DDA New York Class, which was a direct and proximate cause of the Data Breach, and their Private Information being compromised and subsequent harms they suffered;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the

Data Breach, Plaintiffs Gonsalves' and Kavanagh's Private Information and the Private Information of members of the DCA New York Class, DDA New York Class being compromised, and subsequent harms caused to them;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiffs Gonsalves and Kavanagh and members of the DCA New York Class, DDA New York Class, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902 which was a direct and proximate cause of the Data Breach, Plaintiffs Gonsalves' and Kavanagh's Private Information and the Private Information of members of the DCA New York Class, DDA New York Class being compromised, and subsequent harms caused to them;

d. Misrepresenting that they would protect the privacy and confidentiality of the Private Information of Plaintiffs Gonsalves and Kavanagh and members of the DCA New York Class, DDA New York Class, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiffs Gonsalves and Kavanagh and members of the DCA New York Class, DDA New York Class, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902;

f. Omitting, suppressing, and concealing the material fact that they did not properly secure the Private Information of Plaintiffs Gonsalves and Kavanagh and members of the DCA New York Class, DDA New York Class; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of the Private Information of Plaintiffs Gonsalves and Kavanagh and members of the DCA New York Class, DDA New York Class, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902.

2899. DDCA's, DDA's, and DDNY's representations and omissions were material because they were likely to deceive reasonable consumers and clients about the adequacy of their respective data security policies and practices and ability to protect the confidentiality of consumers' Private Information.

2900. Accordingly, Plaintiffs Gonsalves and Kavanagh and members of the DCA New York Class, DDA New York Class acted reasonably in relying on DDCA's, DDA's, and DDNY's misrepresentations and omissions, the truth of which they could not have discovered.

2901. DDCA, DDA, and DDNY acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiffs Gonsalves' and Kavanagh's rights and the rights of members of the DCA New York Class, DDA New York Class.

2902. As a direct and proximate result of DDCA's, DDA's, and DDNY's unfair, unlawful, and/or fraudulent acts and practices, Plaintiffs Gonsalves and Kavanagh and members of the DCA New York Class, DDA New York Class have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for DDCA's, DDA's, and DDNY's dental insurance; loss of the value of access to their Private Information; value of identity and credit protection and repair services made necessary by the Data Breach; and they face ongoing risks of future harms insofar as DDCA, DDA, and DDNY have yet to implement the necessary policies, practices, and measures to adequately safeguard their Private Information in compliance with laws and industry standards.

2903. DDCA's, DDA's, and DDNY's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the many New Yorkers affected by the Data Breach.

2904. The above deceptive and unlawful practices and acts by DDCA, DDA, and DDNY caused substantial injury to New York Delta Dental Bellwether Plaintiffs and New York Subclass Members that they could not reasonably avoid.

2905. Plaintiffs Gonsalves and Kavanagh and members of the DCA New York Class, DDA New York Class seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorneys' fees and costs.

DELTA DENTAL BELLWETHER TWENTY-FIFTH CLAIM FOR RELIEF
Pennsylvania Unfair Trade Practices And Consumer Protection Law ("UTPCPL")
73 Pa. Cons. Stat §§ 201-1, *et seq*.
(On Behalf of DDCA Nationwide Class, or in the alternative, the DDCA Pennsylvania Class; the DDA Nationwide Class, or in the alternative, the DDA Pennsylvania Class; and the DDPenn Nationwide Class, or in the alternative, the DDPenn Pennsylvania Class)

2906. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2907. Plaintiff Marvin Dovberg brings this claim against DDCA on behalf of the DDCA Nationwide Class, or, in the alternative, the DDCA Pennsylvania Class. In addition, Plaintiff Dovberg brings this claim against DDA on behalf of the DDA Nationwide Class, or, in the alternative, the DDA Pennsylvania Class. Plaintiff Dovberg brings this claim against DDPenn on behalf of the DDPenn Nationwide Class, or, in the alternative, the DDPenn Pennsylvania Class.

2908. DDA, DDCA, and DDPenn satisfy the definition of a "person," as meant by 73 Pa. Cons. Stat. § 201-2(2).

2909. Plaintiff Dovberg and DDA, DDCA, and DDPenn Class Members purchased services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes as required by 73 Pa. Cons. Stat. Ann. § 201-9.2(a).

2910. Plaintiff Dovberg and DDA, DDCA, and DDPenn Class Members have a private right of action under Pa. Cons. Stat. Ann. § 201-9.2(a).

2911. DDA, DDCA, and DDPenn engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including the following:

a. Representing that their goods and services have approval, characteristics, uses, or benefits that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

b. Representing that their goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201- 2(4)(vii));

c. Advertising their goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

2912. DDA, DDCA, and DDPenn's unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Dovberg's and DDA, DDCA, and DDPenn Class Members' Private Information, which was a direct and proximate cause of the Data Breach, Plaintiff Dovberg's and DDA, DDCA, and DDPenn Class Members' Private Information being compromised in the Data Breach and subsequent harms;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of Plaintiff Dovberg's and DDA, DDCA, and DDPenn Class Members' Private Information being compromised in the Data Breach and subsequent harms;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Dovberg's and DDA, DDCA, and DDPenn Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902, which was a direct and proximate cause of the Data Breach, DDA, DDCA, and DDPenn Defendants' customers' Private Information being compromised and subsequent harms in the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Dovberg's and DDA, DDCA, and DDPenn Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Dovberg's and DDA, DDCA, and DDPenn Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902;

f. Omitting, suppressing, and concealing the material fact that they did not properly secure Plaintiff Dovberg's and DDA, DDCA, and DDPenn Class Members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Dovberg's and DDA, DDCA, and DDPenn Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; HIPAA, 45 C.F.R. § 164; and HITECH Act, 42 U.S.C. § 17902.

2913. DDA, DDCA, and DDPenn's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of their data security and ability to protect the confidentiality of consumers' Private Information.

2914. DDA, DDCA, and DDPenn intended to mislead Plaintiff Dovberg and DDA, DDCA, and DDPenn Class Members and induce them to rely on its misrepresentations and omissions.

2915. Had DDA, DDCA, and DDPenn disclosed to consumers that they were not complying with industry standards or regulations or that their data systems were not secure and, thus, were vulnerable to attack, they would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law.

2916. DDA, DDCA, and DDPenn were entrusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff Dovberg and DDA, DDCA, and DDPenn Class Members. DDA, DDCA, and DDPenn accepted the responsibility of protecting the data while keeping the inadequate state of their security controls secret from the public. Accordingly, Plaintiff Dovberg and DDA, DDCA, and DDPenn Class Members acted reasonably

in relying on DDA, DDCA, and DDPenn's misrepresentations and omissions, the truth of which they could not have discovered.

2917. DDA, DDCA, and DDPenn acted intentionally, knowingly, and maliciously to violate Pennsylvania's Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff Dovberg's and DDA, DDCA, and DDPenn Class Members' rights.

2918. As a direct and proximate result of DDA, DDCA, and DDPenn's unfair, unlawful, and fraudulent acts and practices, Plaintiff Dovberg and DDA, DDCA, and DDPenn Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for DDCA and Affiliates' dental insurance; loss of the value of access to their Private Information; and the value of identity and credit protection and repair services made necessary by the Data Breach.

2919. Plaintiff Dovberg and DDA, DDCA, and DDPenn Class Members seek all monetary and non-monetary relief allowed by law, including, pursuant to 73 Pa. Stat. Ann. § 201-9.2, actual damages or statutory damages of $100 (whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

DELTA DENTAL BELLWETHER TWENTY-SIXTH CLAIM FOR RELIEF
South Carolina Data Breach Security Act
S.C. Code Ann. §§ 39-1-90, et seq.
(On Behalf of the DDCA South Carolina Class and the DDIC South Carolina Class)

2920. Delta Dental Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Four.

2921. Plaintiff Yvette Tillman brings this claim against DDCA on behalf of the DDCA South Carolina Class. In addition, Plaintiff Tillman brings this claim against DDIC on behalf of the DDIC South Carolina Class.

2922. DDCA and DDIC are each a business that owns or licenses computerized data or other data that includes "personal identifying information" (PII and PHI), as defined by S.C. Code Ann. § 39-1-90(A).

2923. DDCA and DDIC are each a business that owns or licenses computerized data or other data that includes "personal identifying information" (PII and PHI), as defined by S.C. Code Ann. § 39-1-90(A).

2924. Plaintiff Tillman's, DDCA South Carolina Class Members' and DDIC South Carolina Class Members' Private Information includes "personal identifying information" as covered under S.C. Code Ann. § 39-1- 90(D)(3) (for the purpose of this count, "Private Information").

2925. DDCA and DDIC are required to accurately notify Plaintiff Tillman, DDCA South Carolina Class Members, and DDIC South Carolina Class Members following discovery or notification of a breach of its data security systems if Private Information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, in the "most expedient time possible and without unreasonable delay" under S.C. Code Ann. § 39-1-90(A) and (B).

2926. Because DDCA and DDIC discovered a breach of their data security system in which Private Information that was not rendered unusable through encryption, redaction, or other methods, was, or was reasonably believed to have been, acquired by an unauthorized person,

creating a material risk of harm, DDCA and DDIC had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A) and (B).

2927. By failing to disclose the Data Breach in a timely and accurate manner, DDCA and DDIC violated S.C. Code Ann. § 39-1-90(A) and (B).

2928. As a direct and proximate result of DDCA and DDIC's violations of S.C. Code Ann. § 39- 1-90(A), Plaintiff Tillman, DDCA South Carolina Class Members, and DDIC South Carolina Class Members suffered damages, as described above.

2929. Plaintiff Tillman, DDCA South Carolina Class Members, and DDIC South Carolina Class Members seek relief under S.C. Code Ann. § 39-1-90(G), including actual damages, injunctive relief, and attorneys' fees.

IV. PRAYER FOR RELIEF AS AGAINST DELTA DENTAL ENTITIES

2930. Plaintiffs, individually and on behalf of the Delta Dental Bellwether Class, respectfully request that the Court grant the following relief:

a. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiffs as Class Representative and undersigned counsel as Class Counsel;

b. Find in favor of Plaintiffs and the Classes on all counts asserted herein;

c. Award Plaintiffs and the Classes actual, statutory, and/or punitive monetary damages to the maximum extent as allowed by law;

d. Award Plaintiffs and the Classes compensatory, consequential, general, and/or nominal monetary damages in an amount to be proven at trial;

e. Award Plaintiffs and the Classes restitution and all other applicable forms of equitable monetary relief;

f. Award Plaintiffs and the Classes equitable relief by enjoining Delta Dental from engaging in the wrongful conduct complained of herein regarding the misuse or disclosure of the private information of Plaintiffs and Class Members, and by requiring Delta Dental to issue prompt, complete, and accurate disclosure to Plaintiffs and Class Members;

g. Award Plaintiffs and the Classes injunctive relief as permitted by law or equity to assure that they have an effective remedy, and to protect the interests of Plaintiffs and Class Members, including, but not limited to, an order:

i. requiring Delta Dental to protect from unauthorized disclosure all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws, including by adequate encryption of all such data and by preventing unauthorized access to decryption keys;

ii. requiring Delta Dental to delete, destroy, and purge any personal identifying information of Plaintiffs and Class Members in its possession unless Delta Dental can provide to the Court reasonable justification for the retention and use of such information when weighted against the privacy interests of Plaintiffs and Class Members;

iii. requiring Delta Dental to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Delta Dental's systems on a periodic basis, and ordering Delta Dental to promptly correct any problems or issues detected by such third-party security auditors;

iv. requiring Delta Dental to engage independent third-party security auditors and internal personnel to run automated security monitoring including, but not limited to, regular database scanning and securing checks;

v. requiring Delta Dental to audit, test, and train its security personnel regarding any new or modified procedures;

vi. requiring Delta Dental to segment data by, among other things, creating firewalls and access controls so that if one area of Delta Dental network is compromised, hackers cannot gain access to other portions of Delta Dental's systems;

vii. requiring Delta Dental to establish for all Delta Dental employees an information security training program that includes annual training, with additional training to be provided as appropriate;

viii. requiring Delta Dental to establish for all Delta Dental security personnel a security training program that includes regularly scheduled internal training and education to inform Delta Dental's internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

ix. requiring Delta Dental to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Delta Dental's policies, programs, and systems for protecting personal identifying information;

x. requiring Delta Dental to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Delta Dental's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xi. requiring Delta Dental to provide notice to Plaintiffs and all Class Members regarding the full nature and extent of the Data Breach and the disclosure of Private Information to unauthorized persons, including the threat posed as a result of the disclosure of their confidential personal information, and educating Plaintiffs and Class Members regarding steps affected individuals should take to protect themselves;

xii. requiring Delta Dental to implement logging and monitoring programs sufficient to track traffic to and from Delta Dental's servers;

xiii. requiring, for a period of 10 years, the appointment of a qualified and independent third-party assessor to conduct an annual SOC 2 Type 2 attestation to evaluate Delta Dental's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Classes, and to report any deficiencies with compliance of the Court's final judgment;

xiv. requiring Delta Dental to implement multi-factor authentication requirements, if not already implemented; and

xv. requiring Delta Dental employees to employ passwords consistent with best security practices and to change their passwords on a timely and regular basis.

h. Award disgorgement and restitution of all earnings, profits, compensation, and benefits received by Delta Dental as a result of its unlawful acts;

i. Order Delta Dental to purchase or provide funds for lifetime credit monitoring and identify theft insurance to Plaintiffs and Class Members;

j. Order Delta Dental to pay all costs necessary to notice Class Members about the judgment and all costs necessary to administer a court approved claims process.

k. Award Plaintiffs and the Classes pre-judgment and post-judgment interest to the maximum extent allowed by law;

l. Grant Plaintiffs and the Classes leave to amend this complaint to conform to the evidence produced during the course of this case;

m. Award Plaintiffs and the Classes reasonable attorneys' fees, costs, and expenses, as allowable;

n. Where necessary, distribute any monies recovered from Delta Dental on behalf of Class Members or the general public via fluid recovery or cy pres recovery as applicable to prevent Delta Dental from retaining benefits of its wrongful conduct;

o. Award Plaintiffs and the Class such other favorable relief as allowable under law or at equity;

p. Award any other and further relief as may be just and proper; and

q. Conduct a trial by jury on all issues so triable.

CHAPTER FIVE:

FACTUAL ALLEGATIONS AND CAUSES OF ACTION AGAINST MAXIMUS

I. Nature of Maximus' Business

2931. Defendant Maximus, Inc. is the parent of wholly owned subsidiaries Defendants Maximus Federal Services, Inc., Maximus Human Services, Inc., and Maximus Health Services, Inc. (collectively, "Maximus").

2932. Maximus primarily contracts with government agencies to provide services to manage and administer government-sponsored programs, including Medicare and Medicaid. Maximus provides medical evaluations, review of eligibility appeals, enrollment assistance, data analysis, and IT and consulting services.[731] Regarding Medicare specifically, Maximus reviews "more than 600,000 appeals claims a year for Medicare" patients who experienced "health insurance denials."[732]

2933. Maximus is the largest provider of government-sponsored benefit appeals programs in the United States. Maximus currently employs approximately 39,000 individuals and generates more than four billion dollars in annual revenue.[733]

2934. As a condition of performing its services, Maximus requires that its government and corporate customers entrust it with highly sensitive Private Information belonging to Maximus Bellwether Plaintiffs and Class Members.

2935. In its contracts with its government and corporate customers, Maximus agrees to adhere to strict standards of confidentiality regarding the records it maintains. The government

---

[731] *Our Company*, Maximus, https://maximus.com/our-company (last visited Nov. 6, 2024).

[732] *Centers for Medicare and Medicaid*, Maximus, https://maximus.com/cms (last visited Nov. 6, 2024).

[733] *Our Company*, Maximus, https://maximus.com/our-company (last visited Nov. 6, 2024).

requires Maximus to make assurances about its ability to adequately protect data in order to secure its position as a government contractor. For example, in Defendant Maximus Human Services, Inc.'s contract with the State of Tennessee[734] Department of Human Services, Defendant Maximus Human Services, Inc. agreed that "strict standards of confidentiality of records shall be maintained in accordance with State and Federal law and regulations" and that "All material and information provided to [Maximus] … shall be regarded as confidential information" and "[Maximus] agrees to provide safeguards to restrict the use or disclosure of any information concerning such applicants or recipients…."

2936. Maximus uses MOVEit for internal and external file sharing purposes, including to share data with government customers related to Maximus's services in support of certain government programs.[735]

2937. Maximus' website promises consumers that Maximus has robust systems and processes in place to protect and secure their sensitive information.

> Securing every aspect of your mission: We are relentless in our pursuit to protect critical data, operations, and infrastructures. We go beyond traditional security measures to harden enterprise defenses for continuous mission protection.[736]

2938. Maximus's website assures consumers—such as Maximus Bellwether Plaintiffs and Class Members—that Maximus is an "expert" in cybersecurity:

---

[734] *Contract #8, RFS # 345.13-79708, FA # 08-20732-00*, Human Services Child Support Services, State of Tenn. Dept. of Human Resources (Dec. 3, 2009), https://capitol.tn.gov/Archives/Joint/committees/fiscal-review/archives/106ga/contracts/RFS%20345.13-79708%20Human%20Services%20(Maximus%20Human%20Services%20-%20amendment%202).pdf.

[735] *Third Quarter 2024 Form 10-Q*, Maximus, Inc. (Aug. 8, 2024), https://investor.maximus.com/sec-filings/all-sec-filings/content/0001032220-24-000075/0001032220-24-000075.pdf.

[736] *Cybersecurity*, Maximus, https://maximus.com/cybersecurity (last visited Nov. 6, 2024).

> At Maximus, we are relentless in our pursuit of protecting enterprise assets, data, and operations Trusted to manage some of the government's largest security operations, we leverage our deep knowledge of agency mission and extensive technical expertise to create integrated cyber solutions that bolster enterprise cyber defenses for continual mission protection.[737]

2939. Maximus's website repeatedly states that it is keenly cognizant of data privacy risks and has adequate procedures and process in place to prevent them, including its statements that:

a. "We strengthen cyber resiliency, protecting critical data, operations, and infrastructures for continual operational excellence. Our full-spectrum cybersecurity services offer unrivaled cyber defense against the most advanced cyber adversaries. From zero trust to secure application development, we deliver next-gen cyber technologies and solutions that address today's most complex security challenges."[738]

b. "To defend against today's sophisticated cyber adversaries, Maximus goes beyond traditional security measures to harden enterprise security and continuously protect the mission."[739]

c. "Maximus uses various technological and procedural security measures in order to protect the personal information we collect through the Site from loss, misuse, alteration or destruction. We have documented Information Security & Privacy policies to address data protection. We regularly provide information security and privacy awareness training to our employees."[740]

d. "We have prepared a formal incident response plan in case of a data breach."[741]

e. "All employees, including full-time and part-time permanent and temporary employees, complete mandatory data privacy and security training on an annual basis .... We supplement the annual training with ongoing training in multiple mediums. Training topics include, but are not limited, to the

---

[737] *Maximus Cybersecurity Capabilities*, Maximus (2023), *available at* https://maximus.com/sites/default/files/documents/Federal/Maximus_Cybersecurity-Capabilities-Overview.pdf (last visited Nov. 6, 2024).

[738] *Technology Consulting Services*, Maximus, https://maximus.com/technology-consulting-services (last visited Nov. 6, 2024).

[739] *Cybersecurity*, Maximus, https://maximus.com/cybersecurity (last visited Nov. 6, 2024).

[740] *Our Commitment to Privacy*, Maximus, https://maximus.com/privacy-statement (last visited Nov. 6, 2024).

[741] *Id.*

following: • Data protection principles regarding the use, protection, storage, transmission, and disposal of confidential information, with a specific focus on how certain data may not be used."[742]

f. "Maximus developed a robust incident management process to respond to a wide variety of cyber incidents globally. This process includes triage, investigation, evidence collection and storage, root cause analysis, and incident resolution with executive reporting."[743]

2940. Maximus also touts its data security accreditations, including an ISO/IEC 20000-1 certification, and NCQA Accreditation.[744]

2941. Yet, contrary to Maximus's website representations—by virtue of Maximus's admissions that it experienced the Data Breach which revealed the Private Information of more than 11 million individuals—Maximus did not have adequate measures in place to protect and maintain sensitive Private Information entrusted to it or to ensure its vendors and business associates reasonably or adequately secured, safeguarded, and otherwise protected consumers' Private Information that Maximus shared with third-party vendors such as PSC through Maximus's use of MOVEit. Instead, Maximus's website wholly fails to disclose the truth: that Maximus lacks sufficient processes to protect the Private Information that is entrusted to it.

2942. As sophisticated business entities handling highly sensitive and confidential consumer data, Maximus's data security obligations were particularly important, especially in light of the substantial increase in cyberattacks and data breaches in industries handling significant amounts of Private Information preceding the date of the MOVEit Data Breach.

---

[742] *Building a Better Future Together 2023 Sustainability Report*, Maximus, https://sprcdn-assets.sprinklr.com/3774/c8c4202f-e7cb-4d98-aa47-825dc7f8cdbb-2399725906.pdf (last visited Nov. 6, 2024).

[743] *Id.*

[744] *Our Company*, Maximus, https://maximus.com/our-company (last visited Nov. 6, 2024).

2943. In light of recent high profile data breaches—including breaches arising from previously exploited vulnerabilities in other file transfer applications (*e.g.*, Accellion FTA, Fortra GoAnywhere MFT)— at all relevant times, Maximus knew or should have known that its customers', including Maximus Bellwether Plaintiffs, and Class Members', Private Information would be targeted by cybercriminals and ransomware attack groups.

2944. Despite such knowledge, Maximus failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Maximus Bellwether Plaintiffs' and Class Members' Private Information from cyberattacks, including, but not limited to, adequately vetting, auditing, monitoring, testing, and patching the software applications they used to store and transfer such data.

2945. "Third-party software security risks are on the rise, and so are the significant cyber attacks they facilitate. According to a CrowdStrike report, 45% of surveyed organizations said they experienced at least on software supply chain attack in 2021."[745]

2946. Recent high profile cybersecurity incidents at healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), put healthcare partner and provider companies on notice that their electronic records would be targeted by cybercriminals.

[745] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard (last updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software (last visited Dec. 2, 2024).

2947. According to the HIPAA Journal's 2023 Healthcare Data Breach Report, "[a]n unwanted record was set in 2023 with 725 large security breaches in healthcare reported to the Department of Health and Human Services Office for Civil Rights, beating the record of 720 healthcare security breaches set the previous year."[746]

2948. Cyberattacks and data breaches of financial services companies or companies storing financial data are also especially problematic because of the potentially permanent disruption they cause to the daily lives of their customers. Stories of identity theft and fraud abound, with hundreds of millions of dollars lost by everyday consumers every year as a result of internet-based identity theft attacks.[747]

2949. The Government Accountability Office ("GAO") found that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[748]

2950. As highly sophisticated parties that handle sensitive Private Information, Maximus failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Maximus Bellwether Plaintiffs' and Class Members' Private Information.

2951. The ramifications of Maximus' failures to keep Maximus Bellwether Plaintiffs' and Class Members' Private Information secure are severe and long-lasting. To avoid detection,

---

[746] Steve Adler, *Security Breaches in Healthcare in 2023*, THE HIPAA JOURNAL (January 31, 2024), https://www.hipaajournal.com/wp-content/uploads/2024/01/Security_Breaches_In_Healthcare_in_2023_by_The_HIPAA_Journal.pdf (last visited Dec. 2, 2024).

[747] Albert Khoury, *Scam alert: 5 most costly data breaches (plus 5 states most targeted)* (July 27, 2022), https://www.komando.com/security-privacy/most-costly-data-breaches/847800/.

[748] See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown ("GAO Report") at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf [https://perma.cc/GCA5-WYA5].

identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in part because the data can be sold in small batches to multiple buyers as opposed to in bulk to a single buyer. Thus, Maximus Bellwether Plaintiffs and Class Members must vigilantly monitor their financial accounts, and Maximus Bellwether Plaintiffs and Class Members are at an increased risk of fraud and identity theft, for many years into the future.

2952. Thus, Maximus knew, or should have known, the importance of safeguarding the Private Information entrusted to them and of the foreseeable consequences if their systems were breached. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring or from mitigating the consequences of the Data Breach.

2953. As incorporated and realleged herein, Maximus knew of these requirements and of industry cybersecurity standards and their obligations to protect Maximus Bellwether Plaintiffs' and Class Members' highly sensitive Private Information. *See* Chapter One and Chapter Two. Maximus were also aware of the significant repercussions that would result from their failure to do so.

2954. Maximus Bellwether Plaintiffs and Class Members relied Maximus to implement and maintain adequate data security policies and protocols (including vetting, auditing, and monitoring vendors and software companies on which they relied) to keep their Private Information confidential and securely maintained, to use such Private Information (if at all) solely for business and healthcare purposes, and to prevent unauthorized access and disclosure of Private Information to unauthorized persons. Maximus Bellwether Plaintiffs and Class Members reasonably expected Maximus would safeguard their highly sensitive information and keep that Private Information confidential.

2955. In addition to the aforementioned and incorporated industry standards, the Center for Internet Security (CIS) has also published clear guidance on the steps businesses that share information with third parties, *e.g.*, "rely on vendors and partners to help manage their data or rely on third-party infrastructure for core applications or functions," should take to ensure those vendors have appropriate cybersecurity systems and protocols in place, and that their customers' Private Information is adequately safeguarded. Since its formation in 2000, CIS has established applicable industry standards to help people, businesses, and governments protect themselves against pervasive cyber threats that are "globally recognized best practices for security IT systems and data."[749]

2956. Maximus also knew, or should have known, the importance of safeguarding the Private Information entrusted to them, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on affected individuals as a result of a data breach.

2957. Maximus therefore owed a duty to Maximus Bellwether Plaintiffs and Class Members to implement and maintain reasonable and adequate data security measures to secure, protect, and safeguard the Private Information entrusted to them by Maximus Bellwether Plaintiffs and Class Members.

2958. Maximus should have used their resources to implement and maintain adequate data security procedures and practices.

2959. Maximus should have but did not adequately vet Progress or its MOVEit Transfer software, and as a result, failed to prevent or detect the Data Breach.

[749] Center for Internet Security, *Critical Security Controls*, at 12, 42-44 (May 2021), https://perma.cc/R3M4-4KAU] (last visited June 4, 2024).

2960. Maximus knew or should have known that Progress: employed poorly-written, outdated, and insecure code in its MOVEit software; failed to update outdated code; and failed to check for known or newly discovered vulnerabilities.

2961. Maximus failed to ensure Progress employed and maintained adequate cybersecurity measures to prevent the Data Breach from occurring.

2962. Maximus breached their duties to Maximus Bellwether Plaintiffs and Class Members by, among other things, failing to employ adequate screening and vetting practices of its vendors or vendors of its Business Associates, including Progress and its MOVEit Transfer software.

2963. Maximus also had obligations arising under the industry standards, common law, and their own promises and representations made to Maximus Bellwether Plaintiffs and Class Members to keep their Private Information confidential and protected from unauthorized access and disclosure.

II. Maximus Failed to Comply with Industry Standards

2964. Several best practices have been identified that at a minimum should be implemented by entities, like Maximus Defendants, that handle highly sensitive and confidential Private Information.

2965. These best practices include, but are not limited to: educating all employees about data security practices and procedures; requiring strong passwords; implementing multi-layer security—including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without an adequately protected key; multi-factor authentication; backup data; and limiting which employees and third parties can access sensitive data.

2966. Other standard cybersecurity practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email

management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

2967. Maximus failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

2968. These foregoing frameworks are existing and applicable industry standards, and Maximus failed to comply with these accepted standards, thereby opening the door to Cl0p and causing the Data Breach.

III. Had Maximus Taken Its Obligations Seriously, It Would Have Determined that the MOVEit Software was not Safe to Use

2969. Maximus is responsible for protecting the Private Information it solicits and collects from attacks and breaches that result from weaknesses in third-party systems and software.

2970. Maximus failed to safeguard Maximus Bellwether Plaintiffs' and Class Members' Private Information when they failed to adopt and enforce reasonable and available data security practices and procedures to prevent and/or mitigate the known risk of a cyberattack.

2971. Prior to the Data Breach, Maximus should have, but did not, implement and maintain reasonable and necessary data security policies and procedures, which would have mitigated or avoided the Data Breach.

2972. There are numerous known and available steps that Maximus could have taken to mitigate or even prevent the Data Breach.

2973. Data security practices that could and should have been implemented by Maximus to prevent the MOVEit Data Breach include:

a. Auditing of third-party software, including the MOVEit Transfer software;

b. Vetting and periodic auditing of third-party vendors, including Progress;

c. Restricting MOVEit transfers to pre-approved IP addresses ("whitelisting");

d. Limiting the specific types of files that can be uploaded;

e. Conducting basic monitoring of web servers;

f. Using web application firewalls ("WAFs"); and

g. Employing supply chain security.

A. Auditing Third-Party Software

2974. Security audits of third-party software enable companies to identify vulnerabilities, monitor access to sensitive data, and discover and remediate any unauthorized data access.[750] Here, security auditing of the MOVEit Transfer software could have prevented the Data Breach. The methods for conducting security audits of third-party software are well-known and widely available.[751] Maximus therefore could and should have employed companies that conduct security audits of third-party software.[752]

[750] *6 Security Tips for Third Party* Software, Cybersecurity Insiders, https://www.cybersecurity-insiders.com/6-security-tips-for-third-party-software/ (last visited May 20, 2024).

[751] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard (updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software.

[752] Davit Asatryan, *Third-Party Applications Audit: Complete Guide*, Spin.ai (Nov. 4, 2021, updated Apr. 19, 2024), https://spinbackup.com/blog/third-party-applications-audit/.

B. Vetting Vendors

2975. In addition to auditing third-party software, proper vetting and routine audits of vendors' data security practices, including vetting of Progress's cybersecurity practices, could have prevented the Data Breach. Vendor risk assessments or security questionnaires are "one of the best methods for extracting deep cybersecurity insights about any aspects of a vendor's attack surface."[753] Industry-standard risk assessments and security questionnaires designed to help companies discover vulnerabilities in third-party web applications and software are widely available,[754] and can be used to assess the security of third-party software against common attack vectors, including SQL injection susceptibility.[755]

C. Whitelisting

2976. Restricting MOVEit transfers to pre-approved IP addresses—a cybersecurity practice referred to as "whitelisting"—could also have prevented the Data Breach. A whitelist is an administrator-defined register of entities pre-approved for authorized access or to perform specific actions. Whitelisting enhances the security of a system or network by ensuring that only pre-approved users or devices have access to sensitive data or systems. Whitelisting thus denies access by default, providing authorization only to a vetted, pre-approved list of IP addresses, applications, email addresses, and/or users. Blacklisting, in contrast, requires that known threats be specifically identified and blocked, while everything else is permitted. In general, a blacklist is

[753] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard (updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software ("Risk assessments can either be framework-based to identify security control deficiencies against popular security standards or custom-designed for focused investigations about specific third-party risks.").

[754] *Id.*

[755] *Id.*

less effective at protecting against an exploitation of a Zero-Day vulnerability like the one Cl0p exploited in the MOVEit Data Breach than whitelisting. NIST Special Publication 800-167: *Guide to Application Whitelisting* provides specific guidance to companies on how to implement whitelisting.[756]

D. Limiting Specific File Types

2977. Limiting the specific types of files that can be uploaded via FTP could also have prevented the Data Breach. After exploiting the MOVEit vulnerability via SQL injection, Cl0p uploaded the LEMURLOOT web shell, which masqueraded as a legitimate file[757] and allowed the threat actor to execute commands, download files, extract system settings, and create/insert/delete users.[758]

2978. Proper data security dictates that only those files that are needed and expected to be uploaded should be allowed. This typically includes document file types such as .doc, .docx, .pdf, etc. Only web site administrators with whitelisted IP addresses should have been allowed to upload web page files, such as .aspx.

E. Adequate Logging, Monitoring, and Auditing

2979. "Logging, monitoring, and auditing procedures help an organization prevent incidents and provide an effective response when they occur."[759] These tools can detect SQL injection attempts and mitigate or even prevent breaches like the MOVEit Data Breach.

---

[756] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf.

[757] https://blog.qualys.com/vulnerabilities-threat-research/2023/06/07/progress-moveit-transfer-vulnerability-being-actively-exploited; *see also* https://securityintelligence.com/news/the-moveit-breach-impact-and-fallout-how-can-you-respond/.

[758] *#StopRansomware: Cl0p Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, CISA (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[759] Mike Chapple, et al., (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide (9th ed. 2021).

2980. Forensic examinations of the MOVEit Data Breach have confirmed that indicators of compromise were found in the logs of targeted organizations,[760] verifying that effective log monitoring would have mitigated or even prevented the Data Breach. Accordingly, Maximus could and should have utilized commonly available tools that monitor logs automatically and provide alerts of unusual activity to administrators.

2981. "Several different logs record details of activity on systems and networks. For example, firewall logs record details of all traffic that the firewall blocked. By monitoring these logs, it's possible to detect incidents. Some automated methods of log monitoring automatically detect potential incidents and report them right after they've occurred."[761]

2982. Here, adequate logging and log monitoring could have prevented the MOVEit Data Breach because logs would have shown clear indicators of compromise and/or malicious activity. SQL injection attempts, successful or not, will appear in such logs. But even extensive logging is insufficient without adequate monitoring of said logs.

2983. The U.S. National Institute of Standards and Technology (NIST) publishes a Cybersecurity Framework that emphasizes continuous monitoring of systems.[762] The NIST SP 800-92 Guide to Computer Security Log Management further defines how to manage logs,[763] and

[760] Scott Downie, et al., *Transfer Vulnerability (CVE-2023-34362) Since 2021*, Kroll (June 8, 2023), https://www.kroll.com/en/insights/publications/cyber/clop-ransomware-moveit-transfer-vulnerability-cve-2023-34362.

[761] Darril Gibson, CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide, at 73 (2017).

[762] NIST, *The NIST Cybersecurity Framework (CSF) 2*.0, Nat'l Inst. of Standards and Tech. (Feb. 26, 2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[763] NIST, *Guide to Computer Security Log Management*, Nat'l Inst. of Standards and Tech. (Sept. 2006), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf.

there are a number of widely available tools that can monitor logs automatically and provide alerts to administrators when there is unusual activity.

2984. Monitoring web server logs for new files, as recommended in NIST SP 800-12,[764] is a widely accepted cybersecurity practice[765] that would have promptly detected the new files introduced in the MOVEit Data Breach. Web server monitoring would have specifically allowed Maximus to detect the new files introduced to the web server root (human.aspx and human2.aspx) that enabled Cl0p to perpetrate the MOVEit Data Breach. Even basic monitoring of Maximus' web servers could therefore have prevented the Data Breach because it would have revealed the backdoor Cl0p introduced to the web server.[766]

2985. In addition to file system monitoring to identify new files, the InfoSec institute recommends: (a) network monitoring to identify rogue IP addresses which may be performing malicious activities such as brute-force or fuzzing; (b) authentication monitoring to identify unusual logins or login attempts; (c) file change monitoring to identify changes to sensitive files within the file system; and (d) process monitoring to identify rogue processes that might be malicious.[767]

---

[764] NIST, *An Introduction to Information Security*, NIST Special Publication 800-12, Rev. 1 (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

[765] *Monitor web server directories for changed / new files*, https://serverfault.com/questions/1145284/monitor-web-server-directories-for-changed-new-files (last visited May 20, 2024); *Gateway Script to monitor directory for new files*, Ignition https://forum.inductiveautomation.com/t/gateway-script-to-monitor-directory-for-new-files/16124/5 (last visited May 20, 2024).

[766] Tyler Lioi, *MOVEit Transfer Investigations*, CrowdStrike Blog (June 5, 2023), https://www.crowdstrike.com/blog/identifying-data-exfiltration-in-moveit-transfer-investigations/.

[767] Lester Obbayi, *Web server protection: Web server security monitoring*, InfoSec (May 4, 2020), https://www.infosecinstitute.com/resources/network-security-101/web-server-protection-web-server-security-monitoring/.

2986. Beyond monitoring activity, the actual data transferred via MOVEit could and should have been monitored by Maximus. Most legitimate interactions utilizing MOVEit only upload or download relatively small amounts of data at a given time, but Cl0p was able to exfiltrate large amounts of consumer data in the Data Breach. Had Maximus been adequately monitoring data transfers, any attempt to exfiltrate large amounts of data (significantly varying from normal usage) would have triggered an alert.

F. WAFs

2987. Properly configured web application firewalls ("WAFs") could also have prevented or mitigated the effects of the MOVEit Data Breach.[768]

G. Supply Chain Security

2988. Supply chain security is another common method of ensuring that all items in the supply chain, including third-party software like MOVEit, is secure.[769]

2989. The National Institute of Standards and Technology explicitly discusses vulnerabilities in third party software[770] and provides three supply chain security principles[771] that, if applied, would have mitigated or prevented the MOVEit breaches:

---

[768] *See, e.g.*, *Web Application Firewall*, Imperva, https://www.imperva.com/products/web-application-firewall-waf/ (last visited Apr. 26, 2024); Huawei Cloud, *How Does WAF Detect SQL Injection, XSS, and PHP Injection Attacks?* (Sept. 6, 2023), https://support.huaweicloud.com/intl/en-us/waf_faq/waf_01_0457.html.

[769] NIST, *Best Practices in Cyber Supply Chain Risk Management – Conference Materials*, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf (last visited Dec. 3, 2024).

[770] *Id.*

[771] *Id.*

Figure 35

Cyber Supply Chain Security Principles:

1. **Develop your defenses based on the principle that your systems will be breached**. When one starts from the premise that a breach is inevitable, it changes the decision matrix on next steps. The question becomes not just how to prevent a breach, but how to mitigate an attacker's ability to exploit the information they have accessed and how to recover from the breach.
2. **Cybersecurity is never just a technology problem, it's a people, processes and knowledge problem**. Breaches tend to be less about a technology failure and more about human error. IT security systems won't secure critical information and intellectual property unless employees throughout the supply chain use secure cybersecurity practices.
3. **Security is Security.** There should be no gap between physical and cybersecurity. Sometimes the bad guys exploit lapses in physical security in order to launch a cyber attack. By the same token, an attacker looking for ways into a physical location might exploit cyber vulnerabilities to get access.

H. Windows Security Feature

2990. Maximus users utilizing Windows have an additional protection modality. The Windows security system has ransomware protection, which allows the user to designate any folder as protected. Any attempt to add new files or change existing files in that folder would then have to be approved. Because LEMURLOOT masqueraded as a legitimate file that was then used as a backdoor, having the folder \inetpub\wwwroot\ protected from alterations would have prevented these files from being uploaded.

2991. In addition to the foregoing data security practices, which, if adopted by Maximus, could have prevented the Data Breach, there are a number of common security techniques and mechanisms that should be a part of any standard data security policy and could have limited the scope of damage from a data breach. These security techniques and practices include:

a. Limiting access by employing a "least privileges" policy;

b. Implementing "zero-trust" security frameworks;

c. Encrypting data at rest; Immediately applying patches once they were made available.

2992. A "least privileges" policy can limit an attacker who exploits a vulnerability from accessing large volumes of data. Limiting access via policies such as least privileges means that,

even if a threat actor is able to exploit a vulnerability or even use a legitimate login to access the system, access to sensitive data will be limited. The large volume of records accessed and exfiltrated in the Data Breach indicates that this was not done, because it is highly unlikely that any login would have legitimate access to that amount of sensitive data.

2993. "Zero Trust" is a security model and set of system design principles that emphasize security verification in network environments. The core principle of Zero Trust is "never trust, always verify." Thus, unlike traditional security models that assume everything inside a network is safe, Zero Trust assumes threats can exist both inside and outside the network.

2994. Zero Trust security frameworks require all users, whether inside or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted access to applications and data.[772] Numerous standards provide guidelines to organizations implementing "zero-trust" security frameworks, including NIST SP 800-207,[773] NIST SP 800-205,[774] and the CISA zero trust maturity model.[775]

2995. Two aspects of Zero Trust are particularly applicable to the MOVEit Data Breach. The first is the network is segmented into smaller, secure zones to maintain separate access for different parts of the network. This reduces the lateral movement of attackers within the network.

---

[772] *See, e.g.*, *Zero Trust, A revolutionary approach to Cyber or just another buzz word?*, Deloitte (2021), https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/deloitte-cyber-zero-trust.pdf; *see also* Venu Shastri, *Zero Trust Architecture*, CrowdStrike (June 28, 2023), https://www.oracle.com/security/what-is-zero-trust; https://www.crowdstrike.com/cybersecurity-101/zero-trust-security.

[773] NIST, *NIST SP 800-207 – Zero Trust Architecture*, CSRC (Aug. 2020), https://csrc.nist.gov/pubs/sp/800/207/final.

[774] NIST, *NIST SP 800-205 – Attribute Considerations for Access Control Systems*, CSRC (June 2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-205.pdf.

[775] *Zero Trust Maturity Model*, CISA (Apr. 2023), https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf.

The second is continuously monitoring the security posture of all hardware and software on the network. This helps to detect and respond to threats in real time.

2996. The United States Cybersecurity & Infrastructure Security Agency published recommendations for mitigating the MOVEit vulnerability by "[g]rant[ing] admin privileges and access only when necessary, establishing a software allow list that only executes legitimate applications."[776]

2997. Finally, following Progress's announcement of the first MOVEit vulnerability on May 31, 2023,[777] Maximus should have, but did not, immediately begin taking security measures. Maximus' failure to adequately safeguard Maximus Bellwether Plaintiffs' and Class Members' Private Information resulted in that information being accessed or obtained by third-party cybercriminals.

I. Maximus Failed to Follow Progress's Recommendations Regarding Secure Configuration of the MOVEit Software.

2998. The MOVEit software offers secure configurations that any customer could implement to make the system more secure and to mitigate that impact of this breach.

2999. Progress made several additional recommendations to users of the MOVEit software, including:

Using consistency check and tamper check utilities to validate consistently and the audit log.

Review audit logs for any anomalous behavior. Such anomalous behavior includes:

[776] *#StopRansomware: Cl0p Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, CISA (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[777] *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)*, Progress: Community (June 16, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023.

a. Sign-ons from specific IP addresses

b. APIs used

c. Modification of settings

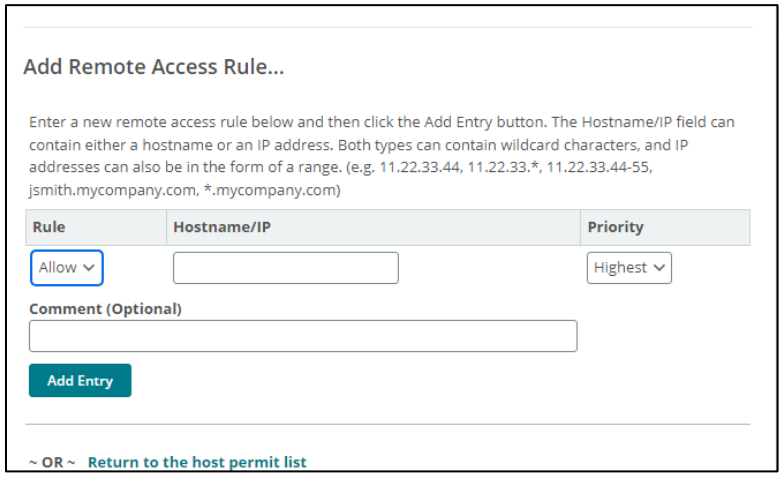
d. Limiting administrative privileges.[778]

e. IP and user lockout policies.[779]

f. Whitelisting so only specific IP addresses and users could login remotely.[780]

3000. Maximus could and should have turned on whitelisting:

Figure 36



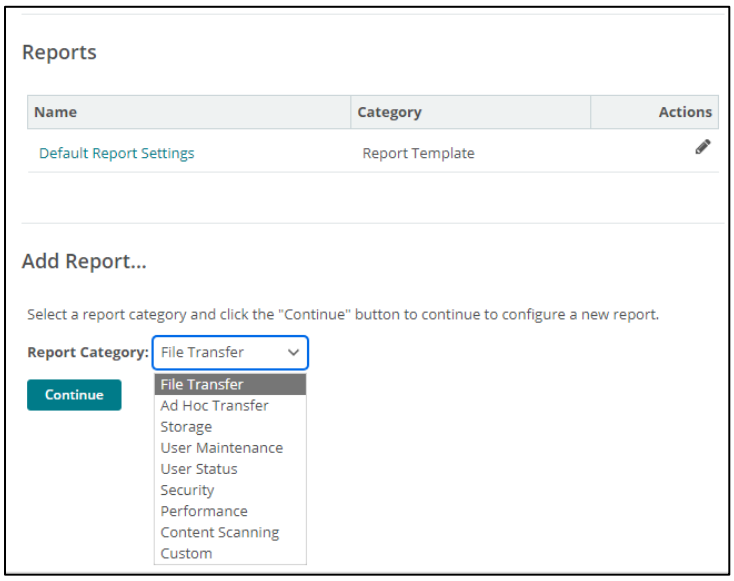
3001. Generating reports in MOVEit is also a simple process:

[778] *Progress Documentation: MOVEit Transfer 2022 Administrator Guide*, Progress (updated Apr. 6, 2022), https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/Permissions_3.html.

[779] *Progress Documentation: MOVEit Automation Web Admin Help – IP/User Lockout Policy*, Progress (updated Feb. 21, 2022), https://docs.progress.com/bundle/moveit-automation-web-admin-help-2022/page/IPUser-Lockout-Policy.html.

[780] *MOVEit Transfer – Whitelist IP for Specific Users Accounts*, Progress: Community (Oct. 14, 2020), https://community.progress.com/s/article/moveit-transfer-whitelist-ip-for-specific-users-accounts.

Figure 37



3002. There are a number of security reports built into the MOVEit software:

Figure 38

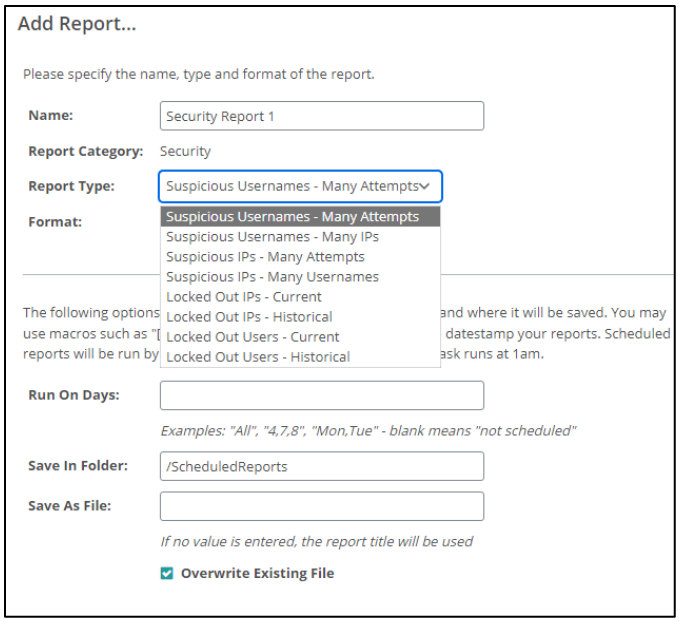
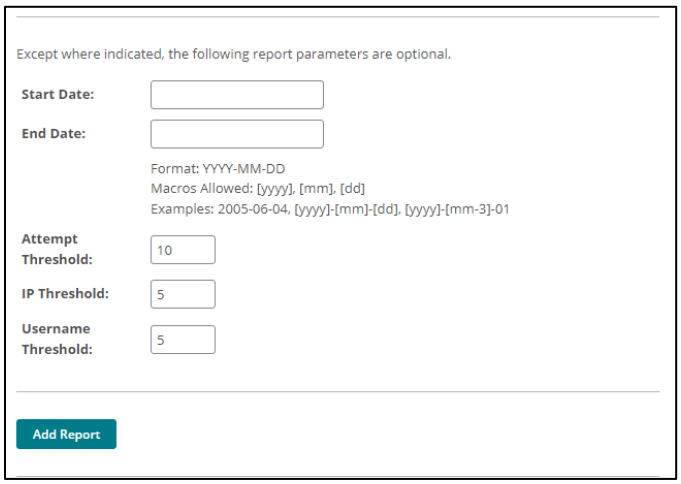
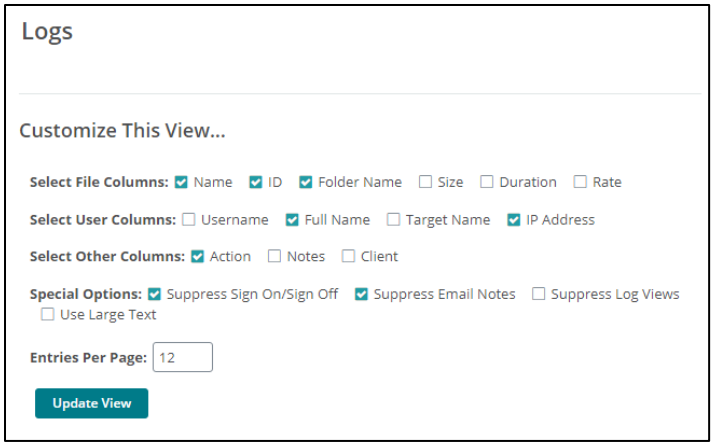


Figure 39



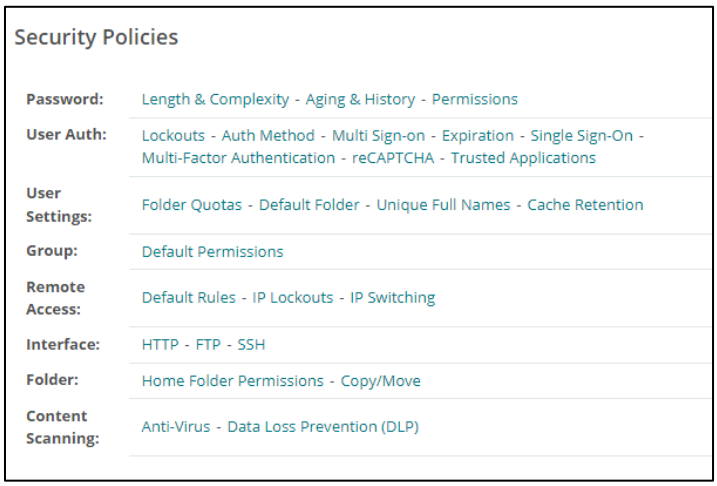
3003. MOVEit users can also customize the view of logs:

Figure 40



3004. A number of additional security policies can be set with a simple point and click:

Figure 41



3005. Data loss prevention rules could and should have been enabled to prevent exfiltration of data:

Figure 42

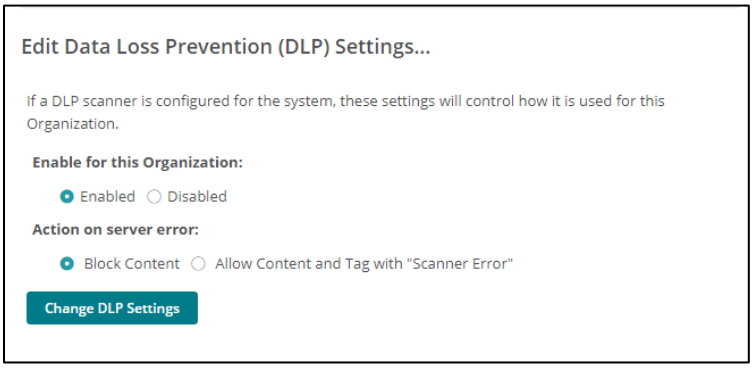


Figure 43

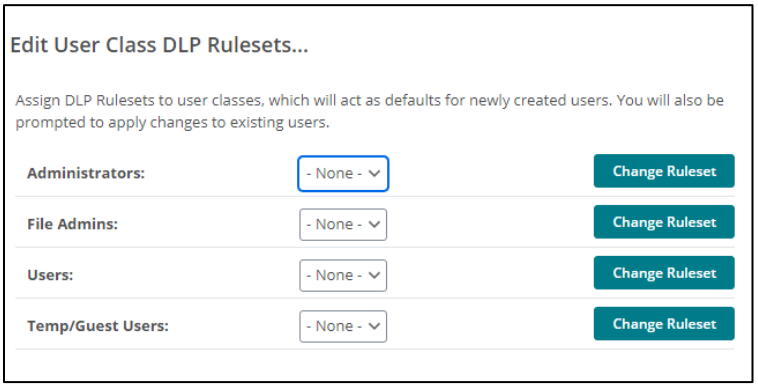
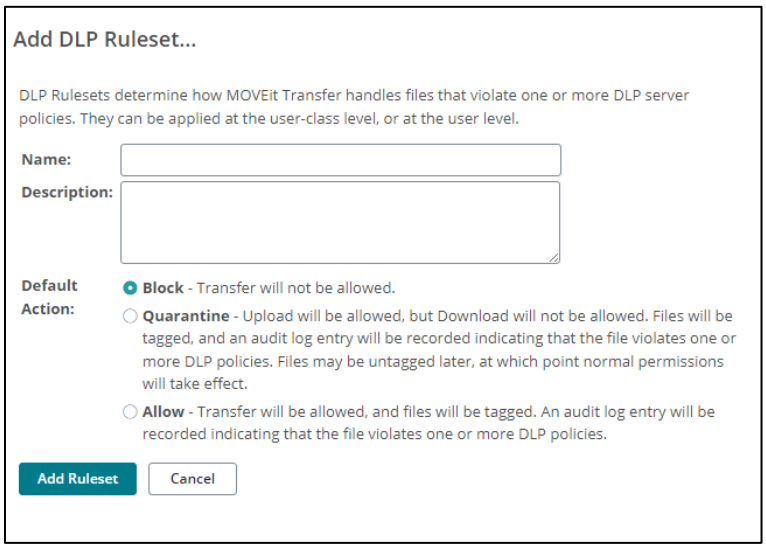


Figure 44



3006. It is unclear which, if any, of these security measures were implemented by Maximus.

J. Maximus Chose to Use the MOVEit Software to Transfer Sensitive Information Despite its Security Flaws.

3007. Maximus enriched themselves by saving the costs they reasonably should have expended on adequate data security measures to secure Maximus Bellwether Plaintiffs' and Class Members' Private Information.

3008. Instead of providing a reasonable level of security that would have prevented the Data Breach, Maximus instead calculated to avoid their data security obligations at the expense of Maximus Bellwether Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Maximus Bellwether Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Maximus Bellwether Defendants' failures to provide the requisite security.

K. Maximus Failed to Protect Maximus Bellwether Plaintiffs' and Class Members' Private Information.

3009. Maximus had a duty to adopt reasonable measures to protect the Private Information of Maximus Bellwether Plaintiffs and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its IT vendors' and affiliates' data security practices and systems. Maximus had a legal duty to keep Private Information safe and confidential.

3010. Maximus had obligations created by the FTC Act, HIPAA, contract, industry standards, representations made to Maximus Bellwether Plaintiffs and Class Members, and common law to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

3011. Maximus derived a substantial economic benefit from collecting Maximus Bellwether Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Maximus could not perform the services it provides.

3012. By obtaining, collecting, using, and deriving a benefit from Maximus Bellwether Plaintiffs' and Class Members' Private Information, Maximus assumed legal and equitable duties and knew or should have known that it was responsible for protecting Maximus Bellwether Plaintiffs' and Class Members' Private Information from disclosure.

IV. CLASS ALLEGATIONS AGAINST MAXIMUS

3013. Maximus Bellwether Plaintiffs Gregory Bloch, S.K. and M.K. (minors through their legal guardian), Robert Plotke, Jvanne Rhodes, and M.P. and M.Y. (minors through their legal guardian) bring this action on behalf of themselves and, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) as representatives of the following Nationwide Class:

> **Maximus, Inc. Nationwide Class**: All residents of the United States whose Private Information was maintained by Maximus, Inc. when it was compromised as a result of the Data Breach.

Plaintiffs Gregory Bloch and S.K. and M.K. (minors through their legal guardian), also bring this action on behalf of themselves and the following Florida Class:

> **Florida Maximus, Inc. Class**: All residents of Florida whose Private Information was maintained by Maximus, Inc. when it was compromised as a result of the Data Breach.

Plaintiff Rob Plotke also brings this action on behalf of himself and the following Illinois Class:

> **Illinois Maximus, Inc. Class**: All residents of Illinois whose Private Information was maintained by Maximus, Inc. when it was compromised as a result of the Data Breach.

Plaintiffs Jvanne Rhodes and M.P. and M.Y. (minors through their legal guardian), also bring this action on behalf of themselves and the following Texas Class:

> **Texas Maximus, Inc. Class**: All residents of Texas whose Private Information was maintained by Maximus, Inc. when it was compromised as a result of the Data Breach.

All of the foregoing classes in this paragraph are collectively referred to as the "Maximus, Inc. Classes," and the foregoing state-specific classes in this paragraph are collectively referred to as the "Maximus, Inc. State Classes."

3014. Maximus Bellwether Plaintiffs Barbara Cruciata, Shellie Harper McCaskell, and Elaine McCoy bring this action on behalf of themselves and, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) as representatives of the following Nationwide Class:

> **MFSI Nationwide Class**: All residents of the United States whose Private Information was maintained by MFSI when it was compromised as a result of the Data Breach.

Plaintiff Barbara Cruciata also brings this action on behalf of herself and the following New York Class:

> **New York MFSI Class**: All residents of New York whose Private Information was maintained by MFSI when it was compromised as a result of the Data Breach.

Plaintiff Shellie McCaskell also brings this action on behalf of herself and the following California Class:

> **California MFSI Class**: All residents of California whose Private Information was maintained by MFSI when it was compromised as a result of the Data Breach.

Plaintiff Elaine McCoy also brings this action on behalf of herself and the following Ohio Class:

> **Ohio MFSI Class**: All residents of Ohio whose Private Information was maintained by MFSI when it was compromised as a result of the Data Breach.

All of the foregoing classes in this paragraph are collectively referred to as the "MFSI Classes," and the foregoing state-specific classes in this paragraph are collectively referred to as the "MFSI State Classes."

3015. Maximus Bellwether Plaintiffs Benjamin Dieck and Victor Diluigi bring this action on behalf of themselves and, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) as representatives of the following Nationwide Class:

> **MSI Nationwide Class**: All residents of the United States whose Private Information was maintained by MSI when it was compromised as a result of the Data Breach.

Plaintiff Ben Dieck also brings this action on behalf of himself and the following North Carolina Class:

> **North Carolina MSI Class**: All residents of North Carolina whose Private Information was maintained by MSI when it was compromised as a result of the Data Breach.

Plaintiff Victor Diluigi also brings this action on behalf of himself and the following Pennsylvania Class:

> **Pennsylvania MSI Class**: All residents of Pennsylvania whose Private Information was maintained by MSI when it was compromised as a result of the Data Breach.

All of the foregoing classes in this paragraph are collectively referred to as the "MSI Classes," and the foregoing state-specific classes in this paragraph are collectively referred to as the "MSI State Classes."

3016. Plaintiff Alexys Taylor brings this action on behalf of herself and, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) as representative of the following Nationwide Class:

> **MHSI Nationwide Class**: "All residents of the United States whose Private Information was maintained by MHSI when it was compromised as a result of the Data Breach".

Plaintiff Alexys Taylor also brings this action on behalf of herself and the following Indiana Class:

> **Indiana MHSI Class**: All residents of Indiana whose Private Information was maintained by MHSI when it was compromised as a result of the Data Breach.

All of the foregoing classes in this paragraph are collectively referred to as the "MHSI Classes."

3017. The foregoing Classes are referred to herein, collectively, as the "Maximus Bellwether Class." The Maximus, Inc. Nationwide Class, the MFSI Nationwide Class, the MSI Nationwide Class, and the MHSI Nationwide Class are herein referred to collectively as the "Nationwide Maximus Classes." The foregoing state-specific Classes are hereinafter referred to collectively as the "Maximus State Classes." Excluded from the Class are: (1) the judges presiding over the action; (2) Maximus, its subsidiaries, parent companies, successors, predecessors, and any entity in which Maximus or its parents have a controlling interest, and its current or former officers and directors; (3) persons who properly opt out; and (4) the successors or assigns of any such excluded persons.

3018. **Numerosity**: Class Members are so numerous that their individual joinder is impracticable, as the proposed Maximus Class includes millions of members who are geographically dispersed.

3019. **Typicality**: Maximus Bellwether Plaintiffs' claims are typical of Class Members' claims. Maximus Bellwether Plaintiffs and all Class Members were injured through Maximus' uniform misconduct, and Plaintiffs' claims are identical to the claims of the Class Members they seek to represent.

3020. **Adequacy**: Maximus Bellwether Plaintiffs' interests are aligned with the Maximus Class they seek to represent and Maximus Bellwether Plaintiffs have retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Maximus Bellwether Plaintiffs and their counsel intend to prosecute this action vigorously. The Maximus Class's interests are well-represented by Maximus Bellwether Plaintiffs and undersigned counsel.

3021. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Maximus Bellwether Plaintiffs' and other Class Members' claims. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class Members individually to effectively redress Maximus' wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents the potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, because of the complex legal and factual issues of the case. By contrast, the class action device

presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

3022. **Commonality and Predominance:** The following questions common to all Class Members predominate over any potential questions affecting individual Class Members:

a. Whether Maximus had a duty to implement and maintain reasonable security procedures and practices to protect and secure Maximus Bellwether Plaintiffs' and Class Members' Private Information from unauthorized access and disclosure;

b. Whether Maximus failed to exercise reasonable care to secure and safeguard Maximus Bellwether Plaintiffs' and Class Members' Private Information;

c. Whether Maximus breached its duties to protect Maximus Bellwether Plaintiffs' and Class Members' Private Information;

d. Whether Maximus violated the statutes alleged herein;

e. Whether Maximus Bellwether Plaintiffs and all other Class Members are entitled to damages and the measure of such damages and relief.

3023. Given that Maximus engaged in a common course of conduct as to Maximus Bellwether Plaintiffs and the Maximus Class, similar or identical injuries and common law violations are involved, and common questions outweigh any potential individual questions.

3024. Unless a Class-wide injunction is issued, Maximus may continue in its failure to properly secure the Private Information of Class Members, Maximus may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Maximus may continue to act unlawfully as set forth in this Petition.

3025. Further, Maximus has acted or refused to act on grounds generally applicable to the Maximus Class and, accordingly, class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

V. CAUSES OF ACTION AGAINST MAXIMUS

MAXIMUS BELLWETHER FIRST CLAIM FOR RELIEF
Negligence
(Brought on Behalf of the Nationwide Maximus Classes, or in the Alternative the Maximus State Classes, Against Maximus)

3026. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3027. Maximus Bellwether Plaintiffs bring this claim against Maximus on behalf of the Maximus Nationwide Classes or, alternatively, the Maximus State Classes.

3028. Maximus knowingly collected, acquired, stored, and/or maintained Maximus Bellwether Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting the Private Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

3029. The duty included obligations to take reasonable steps to prevent disclosure of the Private Information, and to safeguard the information from theft. Maximus' duties included the responsibility to design, implement, and monitor data security systems, policies, and processes to protect against reasonably foreseeable data breaches such as this Data Breach.

3030. Maximus owed a duty of care to Maximus Bellwether Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, policies, and procedures, and the personnel responsible for them, adequately protected the Private Information.

3031. These duties owed by Maximus included the obligation to properly review, assess, and manage the cybersecurity risk posed by third-party vendors and service providers.

3032. Maximus owed a duty of care to safeguard the Private Information due to the foreseeable risk of a data breach and the severe consequences that would result from its failure to so safeguard the Private Information.

3033. Maximus' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Maximus and those individuals who entrusted them with their Private Information, which is recognized by laws and regulations as well as common law. Maximus was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

3034. Under HIPAA, Maximus had a duty to use reasonable security measures to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA. *Id*.

3035. Moreover, under HIPAA, Maximus had a duty to render the electronic Private Information that it maintained as unusable, unreadable, or indecipherable to unauthorized individuals. Specifically, the HIPAA Security Rule requires "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." 45 C.F.R. § 164.304 (defining encryption).

3036. Maximus Bellwether Plaintiffs and Class Members are within the class of persons that the HIPAA was intended to protect. And the injuries that Maximus inflicted on Maximus Bellwether Plaintiffs and Class Members are precisely the harms that HIPAA guards against. After all, the Federal Health and Human Services' Office for Civil Rights ("OCR") has pursued

enforcement actions against businesses which—because of their failure to employ reasonable data security measures—caused the very same injuries that Maximus inflicted upon Maximus Bellwether Plaintiffs and Class Members.

3037. Under § 17932 of the Health Information Technology for Economic and Clinical Health Act ("HITECH"), Maximus has a duty to promptly notify "without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach" the respective covered entities and affected persons so that the entities and persons can take action to protect themselves. 42 U.S.C.A. § 17932(d)(1).

3038. Moreover, § 17932(a) of HITECH states that, "[a] covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (h)(1)) shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach."

3039. And § 17932(b) of HITECH states that, "[a] business associate of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify the covered entity of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach."

3040. Under the Federal Trade Commission Act ("FTCA"), Maximus had a duty to employ reasonable security measures. Specifically, this statute prohibits "unfair . . . practices in or

affecting commerce," including (as interpreted and enforced by the FTC) the unfair practice of failing to use reasonable measures to protect confidential data. 15 U.S.C. § 45.

3041. Moreover, Maximus Bellwether Plaintiffs' and Class Members' injuries are precisely the type of injuries that the FTCA guards against. After all, the FTC has pursued numerous enforcement actions against businesses that—because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the very same injuries that Maximus inflicted upon Maximus Bellwether Plaintiffs and Class Members.

3042. Maximus' duty to use reasonable care in protecting Private Information arose not only as a result of the statutes and regulations described above, but also because Maximus is bound by industry standards to protect Private Information that it acquires, maintains, or stores.

3043. Maximus owed Maximus Bellwether Plaintiffs and Class Members a duty to notify them within a reasonable time frame of any breach to their Private Information. Maximus also owed a duty to timely and accurately disclose to Maximus Bellwether Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. This duty is necessary for Maximus Bellwether Plaintiffs and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of the Data Breach.

3044. Maximus owed these duties to Maximus Bellwether Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Maximus knew or should have known would suffer injury-in-fact from its inadequate security protocols. After all, Maximus actively sought and obtained the Private Information of Maximus Bellwether Plaintiffs and Class Members.

3045. Maximus breached its duties, and thus was negligent, by failing to use reasonable measures to protect Maximus Bellwether Plaintiffs' and Class Members' Private Information. And but for Maximus' negligence, Maximus Bellwether Plaintiffs and Class Members would not have been injured. The specific negligent acts and omissions committed by Maximus include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to comply with—and thus violating—HIPAA and its regulations;

c. Failing to comply with—and thus violating—HITECH and its regulations;

d. Failing to comply with—and thus violating—FTCA and its regulations;

e. Failing to adequately monitor the security of its networks and systems;

f. Failing to have in place mitigation policies and procedures;

g. Allowing unauthorized access to Class Members' Private Information;

h. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

i. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

3046. Maximus breached its duties, and thus was negligent, by failing to use reasonable measures to protect Maximus Bellwether Plaintiffs' and Class Members' Private Information, as alleged and discussed above.

3047. It was foreseeable that Maximus' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Maximus Bellwether Plaintiffs and Class Members.

3048. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the data transfer and storage industry.

3049. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

3050. The imposition of a duty of care on Maximus to safeguard the Private Information it maintained is appropriate because any social utility of Maximus' conduct is outweighed by the injuries suffered by Plaintiffs and Class Members as a result of the Data Breach.

3051. As a direct and proximate result of Maximus' negligence, Maximus Bellwether Plaintiffs and Class Members are at a current and ongoing risk of identity theft, and Maximus Bellwether Plaintiffs and Class Members sustained damages including: (i) invasion of privacy; (ii) financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (iii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iv) financial "out-of-pocket" costs incurred due to actual identity theft; (v) loss of time incurred due to actual identity theft; (vi) loss of time due to increased spam and targeted marketing emails; (vii) loss of value of their Private Information; (viii) future costs of identity theft monitoring; (ix) anxiety, annoyance and nuisance, and (x) the continued risk to their Private Information, which remains in Maximus' control, and which is subject to further breaches, so long as Maximus fails to undertake appropriate and adequate measures to protect Maximus Bellwether Plaintiffs' and Class Members' Private Information.

3052. Maximus Bellwether Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

3053. Maximus' negligent conduct is ongoing, in that it still holds the Private Information of Maximus Bellwether Plaintiffs and Class Members in an unsafe and unsecure manner.

3054. Maximus Bellwether Plaintiffs and Class Members are also entitled to injunctive relief requiring Maximus to (i) strengthen its data security systems and monitoring procedures; (ii)

submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

MAXIMUS BELLWETHER SECOND CLAIM FOR RELIEF
Beach of Third-Party Beneficiary Contract
(Brought on Behalf of the Nationwide Maximus Classes, or in the Alternative the Maximus State Classes, Against Maximus)

3055. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3056. Maximus Bellwether Plaintiffs bring this claim against Maximus on behalf of the Maximus Nationwide Classes or, alternatively, the Maximus State Classes (collectively, the Maximus Class").

3057. Upon information and belief, Maximus entered into contracts with its government and corporate customers to provide administrative services that included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was entrusted to it.

3058. Such contracts were made expressly for the benefit of Maximus Bellwether Plaintiffs and the Class Members, as it was their Private Information that Maximus agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Maximus Bellwether Plaintiffs and the Class were the direct and primary objective of the contracting parties and Maximus Bellwether Plaintiffs and Class Members were direct and express beneficiaries of such contracts.

3059. Maximus knew or should have known that if it were to breach these contracts, Maximus Bellwether Plaintiffs and Class Members would be harmed.

3060. Maximus breached its contracts by, among other things, failing to adequately secure Maximus Bellwether Plaintiffs' and Class Members' Private Information, and, as a result,

Maximus Bellwether Plaintiffs and Class Members were harmed by Maximus' failure to secure their Private Information.

3061. As a direct and proximate result of Maximus' breach, Maximus Bellwether Plaintiffs and Class Members are at a current and ongoing substantial risk of fraud and identity theft, and Maximus Bellwether Plaintiffs and Class Members sustained incidental and consequential damages including: (i) financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out-of-pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) loss of value of their Private Information; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their Private Information, which remains in Maximus's control, and which is subject to further breaches, so long as Maximus fails to undertake appropriate and adequate measures to protect Maximus Bellwether Plaintiffs' and Class Members' Private Information.

MAXIMUS BELLWETHER THIRD CLAIM FOR RELIEF
Unjust Enrichment
(Brought on Behalf of the Nationwide Maximus Classes, or in the Alternative the Maximus State Classes, Against Maximus)

3062. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five, and they bring this claim for relief in the alternative to Maximus Bellwether Plaintiffs' contract-based claims for relief.

3063. Maximus Bellwether Plaintiffs bring this claim against Maximus on behalf of the Maximus Nationwide Classes or, alternatively, the Maximus State Classes (collectively, the Maximus Class").

3064. Maximus Bellwether Plaintiffs and Class Members conferred a monetary benefit on Maximus by providing Maximus with their valuable Private Information.

3065. Maximus enriched itself by saving the costs it reasonably should have expended on data security measures to secure Maximus Bellwether Plaintiffs' and Class Members' Private Information, which cost savings increased the profitability of the services.

3066. Upon information and belief, instead of providing a reasonable level of security that would have prevented the Data Breach, Maximus instead calculated to avoid its data security obligations at the expense of Maximus Bellwether Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Maximus Bellwether Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Maximus' failure to provide the requisite security.

3067. Under the principles of equity and good conscience, Maximus should not be permitted to retain the monetary value of the benefit belonging to Maximus Bellwether Plaintiffs and Class Members, because Maximus failed to implement appropriate data management and security measures that are mandated by industry standards.

3068. Maximus acquired the monetary benefit and Private Information, through inequitable means in that Maximus failed to disclose its inadequate security practices previously alleged.

3069. Had Maximus Bellwether Plaintiffs and Class Members known that Maximus had not secured its Private Information, they would not have agreed to provide their Private Information to Maximus. Maximus Bellwether Plaintiffs and Class Members have no adequate remedy at law.

3070. As a direct and proximate result of Maximus' conduct, Maximus Bellwether Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

3071. Furthermore, as a direct and proximate result of Maximus' unreasonable and inadequate data security practices, Maximus Bellwether Plaintiffs and Class Members are at a current and ongoing risk of identity theft and have sustained incidental and consequential damages, including: (i) financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out-of-pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) loss of value of their Private Information; (vii) future costs of identity theft monitoring; and (viii) the continued risk to their Private Information, which remains in Maximus' control, and which is subject to further breaches, so long as Maximus fails to undertake appropriate and adequate measures to protect Maximus Bellwether Plaintiffs' and Class Members' Private Information.

3072. Maximus Bellwether Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

3073. Maximus Bellwether Plaintiffs and Class Members are also entitled to injunctive relief requiring Maximus to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate ID theft and credit monitoring to all Class Members.

3074. Moreover, Maximus should be compelled to disgorge into a common fund or constructive trust, for the benefit of Maximus Bellwether Plaintiffs and Class Members, proceeds

that it unjustly received from them. In the alternative, Maximus should be compelled to refund the amounts that Maximus Bellwether Plaintiffs and Class Members overpaid for Maximus' services.

MAXIMUS BELLWETHER FOURTH CLAIM FOR RELIEF
Declaratory and Injunctive Relief
(Brought on Behalf of the Nationwide Maximus Classes, or in the Alternative the Maximus State Classes, Against Maximus)

3075. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3076. Maximus Bellwether Plaintiffs bring this claim against Maximus on behalf of the Maximus Nationwide Classes or, alternatively, the Maximus State Classes (collectively, the Maximus Class").

3077. Maximus Bellwether Plaintiffs pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

3078. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

3079. An actual controversy has arisen in the wake of the Data Breach regarding Maximus' present and prospective common law and other duties to reasonably safeguard Maximus Bellwether Plaintiffs' and Class Members' Private Information, and whether Maximus is currently maintaining data security measures adequate to protect Maximus Bellwether Plaintiffs and Class Members from future data breaches that compromise their Private Information. Plaintiffs and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

3080. The Court should also issue prospective injunctive relief requiring Maximus to employ adequate security practices consistent with law and industry standards to protect Maximus Bellwether Plaintiffs' and Class Members' Private Information.

3081. Maximus still controls the Private Information of Maximus Bellwether Plaintiffs and the Class Members.

3082. To Maximus Bellwether Plaintiffs' knowledge, Maximus has made no announcement that it has changed its data or security practices relating to the Private Information.

3083. To Maximus Bellwether Plaintiffs' knowledge, Maximus has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

3084. If an injunction is not issued, Maximus Bellwether Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach. The risk of another such breach is real, immediate, and substantial.

3085. As described above, actual harm has arisen in the wake of the Data Breach regarding Maximus' contractual obligations and duties of care to provide security measures to Maximus Bellwether Plaintiffs and Class Members. Further, Maximus Bellwether Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their Private Information and Maximus' failure to address the security failings that led to such exposure.

3086. There is no reason to believe that Maximus' employee training and security measures are any more adequate now than they were before the Data Breach to meet Maximus' contractual obligations and legal duties.

3087. The hardship to Maximus Bellwether Plaintiffs and Class Members if an injunction does not issue exceed the hardship to Maximus if an injunction is issued. Among other things, if

another data breach occurs, Maximus Bellwether Plaintiffs and Class Members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Maximus of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Maximus has a pre-existing legal obligation to employ such measures.

3088. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the additional injuries that would result to Maximus Bellwether Plaintiffs and the Class.

3089. Maximus Bellwether Plaintiffs and Class Members seek a declaration (i) that Maximus' existing data security measures do not comply with its contractual obligations and duties of care to provide adequate data security; and (ii) that to comply with its contractual obligations and duties of care, Maximus must implement and maintain reasonable security measures, including, but not limited to, the following:

a. engage internal security personnel to conduct testing, including audits on Maximus' systems, on a periodic basis, and promptly correct any problems or issues detected by such third-party security auditors;

b. engage third-party security auditors and internal personnel to run automated security monitoring;

c. audit, test, and train its security personnel and employees regarding any new or modified data security policies and procedures;

d. purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for its provision of services;

e. conduct regular database scanning and security checks; and

f. routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, Private Information.

MAXIMUS BELLWETHER FIFTH CLAIM FOR RELIEF
Invasion of Privacy – Intrusion Upon Seclusion
(Brought on Behalf of the Nationwide Maximus Classes, or in the Alternative the Maximus State Classes, Against Maximus)

3090. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3091. Maximus Bellwether Plaintiffs bring this claim against Maximus on behalf of the Maximus Nationwide Classes or, alternatively, the Maximus State Classes (collectively, the Maximus Class").

3092. Maximus Bellwether Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information that Maximus failed to safeguard and allowed to be accessed by way of the Data Breach.

3093. Maximus' conduct as alleged above intruded upon Maximus Bellwether Plaintiffs' and Class Members' seclusion under common law.

3094. By intentionally and/or knowingly failing to keep Maximus Bellwether Plaintiffs' and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Maximus intentionally invaded Maximus Bellwether Plaintiffs' and Class Members' privacy by:

a. Intentionally and substantially intruding into Maximus Bellwether Plaintiffs' and Class Members' private affairs in a manner that identifies Maximus Bellwether Plaintiffs and Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Maximus Bellwether Plaintiffs and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Maximus Bellwether Plaintiffs and Class Members.

3095. Maximus knew that an ordinary person in Maximus Bellwether Plaintiffs' and Class Members' positions would consider Maximus' intentional actions highly offensive and objectionable.

3096. Maximus invaded Maximus Bellwether Plaintiffs' and Class Members' right to privacy and intruded into Maximus Bellwether Plaintiffs' and Class Members' seclusion by intentionally failing to safeguard, misusing, and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

3097. Maximus intentionally concealed from Maximus Bellwether Plaintiffs and Class Members an incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

3098. As a proximate result of such intentional misuse and disclosures, Maximus Bellwether Plaintiffs' and Class Members' reasonable expectations of privacy in their Private Information were unduly frustrated and thwarted.

3099. Maximus' conduct amounted to a substantial and serious invasion of Maximus Bellwether Plaintiffs' and Class Members' protected privacy interests, causing anguish and suffering such that an ordinary person would consider Maximus' intentional actions or inaction highly offensive and objectionable.

3100. In failing to protect Maximus Bellwether Plaintiffs' and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Maximus acted with intentional malice and oppression and in conscious disregard of Maximus Bellwether Plaintiffs' and Class Members' rights to have such information kept confidential and private.

3101. As a direct and proximate result of Maximus' public disclosure of private facts, Maximus Bellwether Plaintiffs and Class Members are at a current and ongoing risk of identity

theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) loss of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Maximus' possession, and which is subject to further breaches, so long as Maximus fails to undertake appropriate and adequate measures to protect Maximus Bellwether Plaintiffs' and Class Members' Private Information

3102. Maximus Bellwether Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

MAXIMUS BELLWETHER SIXTH CLAIM FOR RELIEF
Invasion of Privacy—Public Disclosure of Private Facts
(Brought on Behalf of the Nationwide Maximus Classes, or in the Alternative the Maximus State Classes, Against Maximus)

3103. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3104. Maximus Bellwether Plaintiffs bring this claim against Maximus on behalf of the Maximus Nationwide Classes or, alternatively, the Maximus State Classes (collectively, the Maximus Class").

3105. Maximus Bellwether Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Maximus mishandled.

3106. As a result of Maximus' conduct, publicity was given to Maximus Bellwether Plaintiffs' and Class Members' Private Information, which necessarily includes matters concerning their private life such as PII and PHI.

3107. A reasonable person of ordinary sensibilities would consider the publication of Maximus Bellwether Plaintiffs' and Class Members' Private Information to be highly offensive.

3108. Maximus Bellwether Plaintiffs' and Class Members' Private Information is not of legitimate public concern and should remain private.

3109. As a direct and proximate result of Maximus' public disclosure of private facts, Maximus Bellwether Plaintiffs and Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) loss of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Maximus' possession, and which is subject to further breaches, so long as Maximus fails to undertake appropriate and adequate measures to protect Maximus Bellwether Plaintiffs' and Class Members' Private Information.

3110. Maximus Bellwether Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

3111. Maximus Bellwether Plaintiffs and Class Members are also entitled to injunctive relief requiring Maximus to, *e.g.*, (i) strengthen its data security systems and monitoring

procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

MAXIMUS BELLWETHER SEVENTH CLAIM FOR RELIEF
Breach of Confidence
(Brought on Behalf of the Nationwide Maximus Classes, or in the Alternative the Maximus State Classes, Against Maximus)

3112. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3113. Maximus Bellwether Plaintiffs bring this claim against Maximus on behalf of the Maximus Nationwide Classes or, alternatively, the Maximus State Classes (collectively, the Maximus Class").

3114. Maximus Bellwether Plaintiffs and Class Members have an interest, both equitable and legal, in Private Information conveyed to, collected by, and maintained by Maximus and ultimately accessed or compromised in the Data Breach.

3115. Maximus has a special relationship with those whose Private Information it maintains, like Maximus Bellwether Plaintiffs and the Class Members.

3116. Because of that special relationship, Maximus was provided with and stored private and valuable Private information related to Maximus Bellwether Plaintiffs and the Class, which it was required to maintain in confidence.

3117. Maximus Bellwether Plaintiffs and the Class provided Maximus with their Private Information under implied agreement of Maximus to limit the use and disclosure of such Private Information.

3118. Maximus owed a duty to Maximus Bellwether Plaintiffs and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting

their Private Information in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

3119. Maximus had an obligation to maintain the confidentiality of Maximus Bellwether Plaintiffs' and the Class Members' Private Information. Maximus Bellwether Plaintiffs and Class Members have a privacy interest in their personal medical matters, and Maximus had a duty not to disclose confidential Private Information.

3120. As a result of the parties' relationship, Maximus had possession and knowledge of confidential Private Information of Maximus Bellwether Plaintiffs and Class Members.

3121. Maximus Bellwether Plaintiffs' and the Class's Private Information is not generally known to the public and is confidential by nature.

3122. Maximus Bellwether Plaintiffs and Class Members did not consent to nor authorize Maximus to release or disclose their Private Information to an unknown criminal actor.

3123. Maximus breached the duties of confidence it owed to Maximus Bellwether Plaintiffs and Class Members when Maximus Bellwether Plaintiffs' and the Class's Private Information was disclosed to unauthorized third parties.

3124. Maximus breached its duties of confidence by failing to safeguard Maximus Bellwether Plaintiffs' and Class Members' Private Information, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to

evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices; (h) storing Private Information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Maximus Bellwether Plaintiffs and the Class Members' Private Information to a criminal third party.

3125. But for Maximus' wrongful breach of its duty of confidences owed to Maximus Bellwether Plaintiffs and Class Members, their privacy, confidences, and Private Information would not have been compromised.

3126. As a direct and proximate result of Maximus' breach of Maximus Bellwether Plaintiffs' and the Class's confidences, Maximus Bellwether Plaintiffs and Class Members have suffered injuries, including: loss of their privacy and confidentiality in their Private Information; costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information; costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach; damages to and loss in value of their Private Information entrusted, directly or indirectly, to Maximus with the mutual understanding that Maximus would safeguard Maximus Bellwether Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others; and mental anguish accompanying the loss of confidences and disclosure of their confidential and Private Information.

3127. As a direct and proximate result of Maximus' breach of its duty of confidences, Maximus Bellwether Plaintiffs and Class Members are entitled to damages, including

compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

MAXIMUS BELLWETHER EIGHTH CLAIM FOR RELIEF
California Consumer Privacy Act ("CCPA")
Cal. Civ. Code § 1798, *et seq*.
(Brought on Behalf of California MFSI Class Against MFSI)

3128. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3129. Maximus Bellwether Plaintiff Shellie Harper McCaskell brings this claim against MFSI on behalf of the California MFSI Class.

3130. The California Legislature has explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[781]

3131. The CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant MFSI failed to implement such procedures which resulted in the Data Breach.

3132. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to

[781] California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/.

the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

3133. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

3134. Maximus Bellwether Plaintiff McCaskell and California MFSI Class members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

3135. Defendant MFSI is a "business" as defined by Civ. Code § 1798.140(c) because it:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

3136. The Private Information at issue is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Maximus Bellwether Plaintiffs' and the California MFSI

Class members' unencrypted first and last names and Social Security numbers among other information.

3137. Maximus Bellwether Plaintiff and California MFSI Class members' Private Information was subject to unauthorized access and exfiltration, theft, or disclosure because their Private Information, including name and contact information was wrongfully taken, accessed, and viewed by unauthorized third parties.

3138. The Data Breach occurred as a result of Defendant MFSI's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Maximus Bellwether Plaintiff McCaskell's and California MFSI Class members' Private Information. Defendant MFSI failed to implement reasonable security procedures to prevent an attack on its server or network, including its email system, by hackers and to prevent unauthorized access of Maximus Bellwether Plaintiff McCaskell's and California MFSI Class members' Private Information as a result of this attack.

3139. On June 11, 2024, Maximus Bellwether Plaintiff McCaskell provided notice to Defendant MFSI pursuant to Cal. Civ. Code § 1798.150(b)(1), identifying the specific provisions of the CCPA Maximus Bellwether Plaintiff McCaskell alleges Defendant MFSI has violated or is violating. Defendant MFSI did not respond to the demand and therefore Maximus Bellwether Plaintiff McCaskell pursues actual or statutory damages as permitted by Cal. Civ. Code § 1798.150(a)(1)(A).

3140. Maximus Bellwether Plaintiff McCaskell seeks all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750) per consumer per incident. See Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

3141. As a result of Defendant MFSI's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Maximus Bellwether Plaintiff McCaskell seeks injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

MAXIMUS BELLWETHER NINTH CLAIM FOR RELIEF
California Consumer Records Act
Cal. Civ. Code § 1798.82, *et seq*.
(Brought on Behalf of California MFSI Class Against MFSI)

3142. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3143. Maximus Bellwether Plaintiff Shellie Harper McCaskell brings this claim against MFSI on behalf of the California MFSI Class.

3144. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay."

3145. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code, § 1798.82(b).

3146. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following information:

i. The name and contact information of the reporting person or business subject to this section;

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

i. The date of the breach;

ii. The estimated date of the breach; or

iii. The date range within which the breach occurred. The notification shall also include the date of the notice.

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

3147. The Data Breach described herein constituted a "breach of the security system" of Defendant MFSI.

3148. As alleged above, Defendant MFSI unreasonably delayed informing Maximus Bellwether Plaintiff McCaskell and California MFSI Class members about the Data Breach, affecting their Private Information, after Defendant MFSI knew the Data Breach had occurred.

3149. Defendant MFSI failed to disclose to Maximus Bellwether Plaintiff McCaskell and the California MFSI Class members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Private Information when Defendant MFSI knew or reasonably believed such information had been compromised.

3150. Defendant MFSI's ongoing business interests gave Defendant MFSI incentive to conceal the Data Breach from the public to ensure continued revenue.

3151. Upon information and belief, no law enforcement agency instructed MFSI that timely notification to Maximus Bellwether Plaintiff McCaskell and the California MFSI Class members would impede its investigation.

3152. As a result of Defendant MFSI's violation of California Civil Code section 1798.82, Maximus Bellwether Plaintiff McCaskell and the California Maximus Federal Services, Inc. Class members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Maximus Bellwether Plaintiff McCaskell and California MFSI Class members because their stolen information would have had less value to identity thieves.

3153. As a result of Defendant MFSI's violation of California Civil Code section 1798.82, Maximus Bellwether Plaintiff McCaskell and the California MFSI Class members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

3154. Maximus Bellwether Plaintiff McCaskell and the California MFSI Class members seek all remedies available under California Civil Code section 1798.84, including, but not limited

to the damages suffered by Maximus Bellwether Plaintiff McCaskell and the other California MFSI Class members, including but not limited to benefit-of-the-bargain and time spent monitoring their accounts for identity theft and medical identity theft, and equitable relief.

3155. Defendant MFSI's misconduct as alleged herein is fraud under California Civil Code section 3294(c)(3) in that it was deceit or concealment of a material fact known to Defendant MFSI conducted with the intent on the part of Defendant MFSI of depriving Maximus Bellwether Plaintiff McCaskell and the California MFSI Class members of "legal rights or otherwise causing injury." In addition, Defendant MFSI's misconduct as alleged herein is malice or oppression under California Civil Code section 3294(c)(1) and (c) in that it was despicable conduct carried on by Defendant MFSI with a willful and conscious disregard of the rights or safety of Maximus Bellwether Plaintiff McCaskell and the California MFSI Class members and despicable conduct that has subjected Maximus Bellwether Plaintiff McCaskell and the California MFSI Class members to cruel and unjust hardship in conscious disregard of their rights. As a result, Maximus Bellwether Plaintiff McCaskell and the California MFSI Class members are entitled to punitive damages against Defendant MFSI under California Civil Code section 3294(a).

MAXIMUS BELLWETHER TENTH CLAIM FOR RELIEF
California Confidentiality of Medical Information Act ("CMIA")
Cal. Civ. Code § 56, *et seq.*
(Brought on Behalf of California MFSI Class Against MFSI)

3156. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3157. Maximus Bellwether Plaintiff McCaskell brings this claim against MFSI on behalf of the California MFSI Class.

3158. Defendant MFSI is a "contractor[s]" as defined in California Civil Code section 56.05(d), and are therefore subject to the requirements of the CMIA, Cal. Civ. Code §56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

3159. As a contractor, Defendant MFSI is required by the CMIA to ensure that medical information regarding patients is not disclosed or disseminated and/or released without patient's authorization, and to protect and preserve the confidentiality of the medical information regarding a patient, under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, 56.36, and 56.101.

3160. Defendant MFSI is required by the CMIA not to disclose medical information regarding a patient without first obtaining an authorization under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, and 56.104.

3161. Defendant MFSI is an entity licensed under California's Business and Professions Code, Division 2.

3162. Maximus Bellwether Plaintiff and California MFSI Class members are "patients" as defined in CMIA, Cal. Civ. Code §56.05(k) ("'Patient' means any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains").

3163. Furthermore, Maximus Bellwether Plaintiff McCaskell and California MFSI Class members had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant MFSI's computer network, and were patients on or before the date of the Data Breach.

3164. Defendant MFSI disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized individuals in the Data Breach

resulted from the affirmative actions of Defendant MFSI's employees, which allowed the hackers to see and obtain Maximus Bellwether Plaintiff's and California MFSI Class members' medical information.

3165. Defendant MFSI negligently created, maintained, preserved, stored, and then exposed Maximus Bellwether Plaintiff McCaskell's and California MFSI Class members' individually identifiable "medical information," within the meaning of Cal. Civ. Code § 56.05(j), including Maximus Bellwether Plaintiff's and California MFSI Class members' names, addresses, medical information, and health insurance information, that alone or in combination with other publicly available information, reveals their identities. Specifically, Defendant MFSI knowingly allowed and affirmatively acted in a manner that allowed unauthorized parties to access, exfiltrate, and actually view Maximus Bellwether Plaintiff's and California MFSI Class members' confidential Private Information.

3166. Defendant MFSI's negligence resulted in the release of individually identifiable medical information pertaining to Maximus Bellwether Plaintiff McCaskell and California MFSI Class members to unauthorized persons and the breach of the confidentiality of that information. Defendant MFSI negligently failed to maintain, preserve, store, abandon, destroy, and/or dispose of Maximus Bellwether Plaintiff McCaskell's and California MFSI Class members' medical information in a manner that preserved the confidentiality of the information contained therein, in violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

3167. Defendant MFSI also violated Sections 56.06 and 56.101 of the CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction, or disposal of confidential personal medical information.

3168. Maximus Bellwether Plaintiff McCaskell's and California MFSI Class members' medical information was accessed and actually viewed by hackers in the Data Breach.

3169. Maximus Bellwether Plaintiff McCaskell's and California MFSI Class members' medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

3170. Defendant MFSI's computer systems did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code § 56.101(b)(1)(A). As a direct and proximate result of Defendant MFSI's above-noted wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Maximus Bellwether Plaintiff McCaskell and the California MFSI Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia:

a. present, imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud –risks justifying expenditures for protective and remedial services for which they are entitled to compensation;

b. invasion of privacy;

c. breach of the confidentiality of the Private Information;

d. statutory damages under the California CMIA;

e. loss of the value of their Private Information, for which there is well-established national and international markets; and/or,

f. the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

3171. As a direct and proximate result of Defendant MFSI's wrongful actions, inactions, omissions, and want of ordinary care that directly and proximately caused the release of Maximus

Bellwether Plaintiff McCaskell's and California MFSI Class members' Private Information, Maximus Bellwether Plaintiff McCaskell's and California MFSI Class members' personal medical information was viewed by, released to, and disclosed to third parties without Maximus Bellwether Plaintiff McCaskell's and California MFSI Class members' written authorization.

3172. Defendant MFSI's negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Maximus Bellwether Plaintiff McCaskell's and California MFSI Class members' medical information in a manner that preserved the confidentiality of the information contained therein violated the CMIA.

3173. Maximus Bellwether Plaintiff McCaskell and the California MFSI Class members were injured and have suffered damages, as described above, from Defendant MFSI's illegal and unauthorized disclosure and negligent release of their medical information in violation of Cal. Civ. Code §§56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, which allows for actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorneys' fees, expenses, and costs.

MAXIMUS BELLWETHER ELEVENTH CLAIM FOR RELIEF
California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.*
(Brought on Behalf of California MFSI Class Against MFSI)

3174. Maximus Bellwether Plaintiffs Shellie reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3175. Maximus Bellwether Plaintiff McCaskell brings this claim against MFSI on behalf of the California MFSI Class.

3176. Defendant MFSI regularly does business in California. Defendant MFSI violated California's Unfair Competition Law ("UCL") (Cal. Bus. & Prof. Code, § 17200, et seq.) by

engaging in unlawful, unfair, or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

a. by representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Private Information from unauthorized disclosure, release, data breach, and theft; representing and advertising that it did and would comply with the requirement of relevant federal and state laws pertaining to the privacy and security of the California class members' Private Information; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Private Information;

b. by soliciting and collecting California MFSI Class members' Private Information with knowledge that the information would not be adequately protected; and by storing Maximus Bellwether Plaintiff's McCaskell and California MFSI Class members' Private Information in an unsecure electronic environment;

c. by failing to disclose the Data Breach in a timely and accurate manner, in violation of California Civil Code section 1798.82;

d. by violating the privacy and security requirements of HIPAA, 42 U.S.C. §1302d, *et seq*.;

e. by violating the CMIA, California Civil Code section 56, *et seq*.; and

f. by violating the CCRA, California Civil Code section 1798.82.

3177. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Maximus Bellwether Plaintiff McCaskell and California MFSI Class members. Defendant MFSI's practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq.*, CMIA, Cal. Civ. Code, § 56, *et seq.*, and the CCRA, Cal. Civ. Code, § 1798.81.5.

3178. As a direct and proximate result of Defendant MFSI's unfair and unlawful practices and acts, Maximus Bellwether Plaintiff McCaskell and the California MFSI Class members were injured and lost money or property, including but not limited to the overpayments Defendant MFSI received to take reasonable and adequate security measures (but did not), the loss of their legally protected interest in the confidentiality and privacy of their Private Information, and additional losses described above.

3179. Defendant MFSI knew or should have known that its computer systems and data security practices were inadequate to safeguard Maximus Bellwether Plaintiff McCaskell's and California MFSI Class members' Private Information and that the risk of a data breach or theft was highly likely. Defendant MFSI's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff McCaskell and the California MFSI Class members.

3180. Maximus Bellwether Plaintiff McCaskell seeks relief under the UCL, including restitution to the California MFSI Class members of money or property that the Defendant MFSI may have acquired by means of Defendant MFSI's deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. Proc., § 1021.5), and injunctive or other equitable relief.

MAXIMUS BELLWETHER TWELFTH CLAIM FOR RELIEF
California Constitution's Right to Privacy
Cal. Const., Art. I, § I
(Brought by Plaintiff McCaskill on Behalf of the California MFSI Class Against MFSI)

3181. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3182. Plaintiff McCaskell brings this claim against MFSI on behalf of the California MFSI Class.

3183. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

3184. The right to privacy in California's Constitution creates a private right of action against private and government entities.

3185. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

3186. MFSI violated Plaintiff McCaskell's and the California MFSI Class Members' constitutional right to privacy by facilitating the collection and storage of their Private Information and by then disclosing, or preventing from unauthorized disclosure, their Private Information, which includes information in which they had a legally protected privacy interest, and for which they had a reasonable expectation of privacy. Disclosure of their Private Information was highly offensive given the highly sensitive nature of the data. Disclosure of their private medical information in particular could cause humiliation to Plaintiff McCaskell and the California MFSI Class Members. Accordingly, disclosure of their Private Information is an egregious violation of social norms.

3187. MFSI intruded upon Plaintiff McCaskell's and the California MFSI Class Members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential Private Information.

3188. Plaintiff McCaskell and the California MFSI Class Members had a reasonable expectation of privacy in that: (i) their invasion of privacy occurred as a result of MFSI's lax and inadequate security practices with respect to securely developing and maintaining its MOVEit software, which facilitated the collection, storage, and use of Plaintiff McCaskell's and the California MFSI Class Members' data, as well as with respect to preventing the unauthorized disclosure of their Private Information; (ii) Plaintiff McCaskell and the California MFSI Class Members did not consent or otherwise authorize MFSI to disclose their Private Information to parties responsible for the cyberattack; and (iii) Plaintiff McCaskell and the California MFSI Class Members could not reasonably expect MFSI would commit acts in violation of laws protecting their privacy.

3189. As a result of MFSI's actions, Plaintiff McCaskell and the California MFSI Class Members have been damaged as a direct and proximate result of MFSI's invasion of their privacy and are entitled to just compensation.

3190. Plaintiff McCaskell and the California MFSI Class Members suffered actual and concrete injury as a result of MFSI's violations of their privacy interests. Plaintiff McCaskell and the California MFSI Class Members are entitled to appropriate relief, including damages to compensate them for the harms to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by MFSI's invasions.

3191. Plaintiff McCaskell and the California MFSI Class Members seek appropriate relief for that injury, including, but not limited to, damages that will reasonably compensate them for the harm to their privacy interests as well as disgorgement of profits made by MFSI as a result of their intrusions upon Plaintiff McCaskell's and the California MFSI Class Members' privacy.

MAXIMUS BELLWETHER THIRTEENTH CLAIM FOR RELIEF
Violation of Massachusetts General Laws, Chapter 93A
(Brought on behalf of the Maximus Nationwide Classes or, in the alternative, the Maximus State Classes)

3192. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3193. Maximus Bellwether Plaintiffs bring this claim against Maximus on behalf of the Maximus Nationwide Classes or, in the alternative, the Maximus State Classes.

3194. M.G.L. ch. 93A §§ 2 and 9. M.G.L. ch. 93A § 2 provides that "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." M.G.L. ch. 93A § 9 permits any consumer injured by a violation of M.G.L. ch. 93A § 2 to bring a civil action, including a class action, for damages and injunctive relief.

3195. Maximus Bellwether Plaintiffs allege that Maximus committed unfair business acts and/or practices in violation of M.G.L. ch. 93A §§ 2 and 9.

3196. Maximus knew or should have known of the inherent risks in experiencing a data breach if it failed to maintain adequate systems and processes for keeping Maximus Bellwether Plaintiffs' and Class Members' PII safe and secure. Only Maximus was in a position to ensure that its systems were sufficient to protect against harm to Maximus Bellwether Plaintiffs and Class

Members resulting from a data security incident such as the Data Breach; instead, it failed to implement such safeguards.

3197. Maximus' own conduct also created a foreseeable risk of harm to Maximus Bellwether Plaintiffs and Class Members and their PII. Maximus' misconduct included failing to adopt, implement, and maintain the systems, policies, and procedures necessary to prevent the Data Breach.

3198. Maximus acknowledges its conduct created actual harm to Maximus Bellwether Plaintiffs and Class Members because Maximus instructed them to monitor their accounts for fraudulent conduct and identity theft.

3199. Maximus knew, or should have known, of the risks inherent in disclosing, collecting, storing, accessing, and transmitting PII and the importance of adequate security because of, *inter alia*, the prevalence of data breaches.

3200. Maximus failed to adopt, implement, and maintain fair, reasonable, or adequate security measures to safeguard Maximus Bellwether Plaintiffs' and Class Members' PII, failed to recognize the Data Breach in a timely manner, and failed to notify Maximus Bellwether Plaintiffs and Class Members in a timely manner that their PII was accessed in the Data Breach.

3201. These acts and practices are unfair in material respects, offend public policy, are immoral, unethical, oppressive and unscrupulous and violate 201 CMR 17.00 and M.G.L. ch. 93A § 2.

3202. As a direct and proximate result of Maximus' unfair acts and practices, Maximus Bellwether Plaintiffs and Class Members have suffered injury and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the publication and/or fraudulent use of their PII; (iii) out-of-pocket

expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from unemployment and/or tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Maximus' possession (and/or to which Maximus continues to have access) and is subject to further unauthorized disclosures so long as Maximus fails to undertake appropriate and adequate measures to protect the PII in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of disclosed PII.

3203. Neither Maximus Bellwether Plaintiffs nor Class Members contributed to the Data Breach.

3204. Maximus Bellwether Plaintiff Barbara Cruciata sent a demand for relief, in writing, to Maximus as required by M.G.L. ch. 93A § 9 on or about August 23, 2023, prior to filing this complaint.[782] Maximus Bellwether Plaintiffs have not received a written tender of settlement that is reasonable in relation to the injury actually suffered by Maximus Bellwether Plaintiffs and Class Members.

3205. Based on the foregoing, Maximus Bellwether Plaintiffs and Class Members are

[782] *See, e.g.*, *Ghalem, et al. v. Progress Software Co., et al.*, 23-cv-12300 (D. Mass.), at ECF No. 1, ¶ 213 ("A demand identifying the claimant and reasonably describing the unfair or deceptive act or practice relied upon and the injury suffered was mailed or delivered to Defendants at least thirty days prior to the filing of a pleading alleging this claim for relief").

entitled to all remedies available pursuant to M.G.L ch. 93A, including, but not limited to, refunds, actual damages, or statutory damages in the amount of twenty-five dollars per violation, whichever is greater, double or treble damages, attorneys' fees and other reasonable costs.

3206. Pursuant to M.G.L. ch. 231, § 6B, Maximus Bellwether Plaintiffs and Class Members are further entitled to pre-judgment interest as a direct and proximate result of Maximus' wrongful conduct. The amount of damages suffered as a result is a sum certain and capable of calculation and Maximus Bellwether Plaintiffs and Class Members are entitled to interest in an amount according to proof.

MAXIMUS BELLWETHER FOURTEENTH CLAIM FOR RELIEF
New York Deceptive Trade Practices Act ("GBL")
N.Y. Gen. Bus. Law. § 349
(Brought on behalf of the New York MFSI Class)

3207. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3208. Plaintiff Barbara Cruciata brings this claim against MFSI on behalf of the New York MFSI Class.

3209. Maximus Federal Services, Inc conducts substantial business in the state of New York.

3210. Maximus Federal Services, Inc engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Cruciata's and New York Maximus Federal Services, Inc Class Members' PII, which was a direct and proximate cause of the Data Breach, their PII being compromised, and subsequent harms caused to Plaintiff Cruciata and New York MFSI Class;

b. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach, Plaintiff Cruciata's and New York MFSI Class Members' PII being compromised, and subsequent harms caused to Plaintiff Cruciata and the New York MFSI Class;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Cruciata's and New York MFSI Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach, Plaintiff Cruciata's and New York MFSI Members' PII being compromised, and subsequent harms caused to Plaintiff Cruciata and the New York MFSI Class;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Cruciata's and the New York MFSI's PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Cruciata and the New York MFSI Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff Cruciata's and the New York MFSI Class Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Cruciata's and New York MFSI Class Members' PII, including duties imposed by the FTCA, 15 U.S.C. § 45.

3211. MFSI's representations and omissions were material because they were likely to deceive reasonable consumers and clients about the adequacy of its data security policies and practices and ability to protect the confidentiality of consumers' PII.

3212. Accordingly, Plaintiff Cruciata and New York MFSI Class Members acted reasonably in relying on MFSI's misrepresentations and omissions, the truth of which they could not have discovered.

3213. MFSI acted intentionally, knowingly, and maliciously to violate New York's

General Business Law, and recklessly disregarded Plaintiff Cruciata's and New York MFSI Class Members' rights.

3214. As a direct and proximate result of MFSI's unfair, unlawful, and/or fraudulent acts and practices, Plaintiff Cruciata and New York MFSI Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for products and services; loss of the value of access to their PII; value of identity and credit protection and repair services made necessary by the Data Breach; and they face ongoing risks of future harms insofar as they have yet to implement the necessary policies, practices, and measures to adequately safeguard their PII in compliance with laws and industry standards.

3215. MFSI's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the many New Yorkers affected by the Data Breach.

3216. The above deceptive and unlawful practices and acts by MFSI caused substantial injury to Plaintiff Cruciata and New York MFSI Class Members that they could not reasonably avoid.

3217. Plaintiff Cruciata and New York MFSI Class Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorneys' fees and costs.

MAXIMUS BELLWETHER FIFTEENTH CLAIM FOR RELIEF
North Carolina Identity Theft Protection Act
N.C. Gen. Stat. Ann. § 75-1.1
(Brought on behalf of the North Carolina MSI Class)

3218. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3219. Plaintiff Ben Dieck brings this claim against MSI on behalf of the North Carolina MSI Class (the "North Carolina Class").

3220. MSI is a business that owns or licenses computerized data that includes Private Information as defined by N.C. Gen. Stat. § 75- 61(1).

3221. Plaintiff Dieck and North Carolina MSI Class Members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

3222. MSI is required to accurately notify Plaintiff Dieck and North Carolina MSI Class Members if it discovers a security breach or receives notice of a security breach (where unencrypted and unredacted Private Information was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. § 75-65.

3223. Plaintiff Dieck's and North Carolina MSI Class Members' Private Information includes information as covered under N.C. Gen. Stat. § 75-61(10).

3224. Because MSI discovered a security breach and had notice of a security breach (where unencrypted and unredacted Private Information was accessed or acquired by unauthorized persons), MSI had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

3225. By failing to disclose the Data Breach in a timely and accurate manner, MSI violated N.C. Gen. Stat. § 75-65.

3226. MSI, as a provider of government-sponsored benefit appeals programs, was entrusted with highly sensitive Private Information, and had actual knowledge Plaintiff Dieck and North Carolina MSI Class Members would not want this information disclosed.

3227. Additionally, under N.C. Gen. Stat. § 75-66(e) MSI violated the provisions on publishing personal information in N.C. Gen. Stat. § 1-539.2C.

3228. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. Art. 2A § 75-1.1.

3229. As a direct and proximate result of MSI's violations of N.C. Gen. Stat. § 75-65, § 75-66(e), and § 1-539.2C, Plaintiff Dieck and North Carolina MSI Class Members suffered damages, as alleged above.

3230. Plaintiff Dieck and North Carolina MSI Class Members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, § 75-66(e), and § 1-539.2C which provides damages for identity theft between $500 and $5000 per violation, and including treble damages, and attorneys' fees.

MAXIMUS BELLWETHER SIXTEENTH CLAIM FOR RELIEF
North Carolina Unfair and Deceptive Trade Practices Act
N.C. Gen. Stat. Ann. § 75-1.1, *et seq.*
(Brought on behalf of the North Carolina MSI Class)

3231. Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3232. Plaintiff Ben Dieck brings this claim against MSI on behalf of the North Carolina MSI Class.

3233. MSI sells and performs services in North Carolina and engaged in commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

3234. MSI engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Dieck's and North Carolina MSI Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to implement and maintain reasonable security and privacy measures to protect against unauthorized access to or use of Plaintiff Dieck's and North Carolina MSI Class Members' Private Information in connection with or after its disposal in violation of §75-64(f), which was a direct and proximate cause of the Data Breach;

c. Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Dieck's and North Carolina MSI Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Dieck's and North Carolina MSI Class Members' Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Dieck's and North Carolina MSI Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or properly secure Plaintiff Dieck's and North Carolina MSI Class Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Dieck's and North Carolina MSI Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

3235. MSI's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of a MSI's data security and ability to protect the confidentiality of consumers' Private Information.

3236. MSI intended to mislead Plaintiff Dieck and North Carolina MSI Class Members and induce them to rely on its misrepresentations and omissions.

3237. MSI was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff Dieck and North Carolina MSI Class Members. MSI accepted the responsibility of maintaining, storing and protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff Dieck and North Carolina MSI Class Members acted reasonably in relying on MSI's misrepresentations and omissions, the truth of which they could not have discovered.

3238. MSI acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff Dieck's and North Carolina MSI Class Members' rights.

3239. As a direct and proximate result of MSI's unfair and deceptive acts and practices, Plaintiff Dieck and North Carolina MSI Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for MSI's services; loss of the value of access to their Private Information; and the value of identity protection services made necessary by the Data Breach.

3240. MSI's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

3241. Plaintiff Dieck and North Carolina MSI Class Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

MAXIMUS BELLWETHER SEVENTEENTH CLAIM FOR RELIEF
Violations Of The Pennsylvania Unfair Trade Practices And Consumer Protection Law ("UTPCPL"), 73 P.S. §§ 201-1–201-9.3
(Brought on behalf of the Pennsylvania MSI Class)

3242. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3243. Plaintiff Diluigi brings this claim against MSI on behalf of the Pennsylvania MSI Class.

3244. MSI sells and performs services in the Commonwealth of Pennsylvania.

3245. Plaintiff Diluigi, Pennsylvania MSI Class Members, and MSI are "persons" as defined by the UTPCPL. 73 P.S. § 201-2(2).

3246. MSI's products and services constitute as "trade" and "commerce" under the statute. 73 P.S. § 201-2(3).

3247. MSI obtained Plaintiff Diluigi's and Pennsylvania MSI Class Members' PII in connection with the services it performs and provides.

3248. MSI engaged in unfair or deceptive acts in violation of the UTPCPL by failing to implement and maintain reasonable security measures to protect and secure consumers' (such as Plaintiff Diluigi and Pennsylvania MSI Class Members') PII in a manner that complied with

applicable laws, regulations, and industry standards, including by failing to control all environments into which it placed consumers' PII, and to ensure that those environments were used, configured and monitored in such a way as to ensure the safety of consumers' data.

3249. As alleged above, MSI made explicit statements to its customers that their PII will remain private and secure.

3250. The UTPCPL lists twenty-one instances of "unfair methods of competition" and "unfair or deceptive acts or practices." 73 P.S. § 201-2(4). MSI's failure to adequately protect Plaintiff Diluigi's and Pennsylvania MSI Class Members' PII while holding out that it would adequately protect the PII falls under at least the following categories:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation or connection that he does not have (73 P.S. § 201-2(4)(v));

b. Representing that goods or services are of a particular standard, quality or grade, or that goods are of a particular style or model, if they are of another (73 P.S. § 201-2(4)(vii));

c. Advertising goods or services with intent not to sell them as advertised (73 P.S. § 201-2(4)(ix)); and

d. Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding (73 P.S. § 201-2(4)(xxi)).

3251. Due to the Data Breach, Plaintiff Diluigi and Pennsylvania MSI Class Members have lost property in the form of their PII. Further, Maximus Human Services, Inc's failure to adopt reasonable practices in protecting and safeguarding its customers' PII will force Plaintiff Diluigi and Pennsylvania MSI Class Members to spend time or money to protect against identity theft. Plaintiff Diluigi and Pennsylvania MSI Class Members are now at a higher risk of identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for MSI's practices of collecting and storing PII without appropriate and reasonable safeguards to protect

such information.

3252. As a result of MSI's violations of the UTPCPL, Plaintiff Diluigi and Pennsylvania MSI Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased or imminent risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost value of the unauthorized access to their PII permitted by MSI; (vi) the value of long-term credit monitoring and identity theft protection products necessitated by the Data Breach; (vii) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (viii) overpayment for the services that were received without adequate data security.

3253. Pursuant to 73 P.S. § 201-9.2(a), Plaintiff Diluigi and Pennsylvania MSI Class Members seek actual damages, $100, or three times their actual damages, whichever is greatest. Plaintiff Diluigi and Pennsylvania MSI Class Members also seek costs and reasonable attorney fees.

MAXIMUS BELLWETHER COUNT XV
VIOLATIONS OF ILLINOIS PERSONAL INFORMATION PROTECTION ACT ("PIPA"), 815 ILCS 530/10(a)
(Brought on behalf of the Illinois Maximus, Inc. Class)

3254. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3255. Plaintiff Plotke brings this claim against Maximus, Inc. on behalf of the Illinois Maximus, Inc. Class.

3256. Section 10(b) of PIPA states, in pertinent part:

> [a]ny data collector that maintains or stores, but does not own or license, computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

815 ILCS 530/10(b).

3257. Maximus, Inc. conducts substantial business in Illinois.

3258. Maximus, Inc. is a "data collector" as defined by the statute because it "handles, collects, disseminates, or otherwise deals with nonpublic personal information." 815 ILCS 530/5.

3259. Plaintiff Plotke and the Illinois Maximus, Inc. Class Members' claims are based on their statuses as "owner[s]" of their PII.

3260. Maximus, Inc. failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach.

3261. Section 45 of PIPA requires entities who maintain or store "personal information concerning an Illinois resident" to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure."

3262. Maximus, Inc.'s conduct violated PIPA because it voluntarily undertook the act of maintaining and storing Plaintiff Plotke's PII, but failed to implement safety and security procedures and practices sufficient enough to protect the PII from the Data Breach that it should have anticipated.

3263. Maximus, Inc. should have known and anticipated that data breaches were on the rise and that software companies were lucrative or likely targets of cyber criminals looking to steal PII. Therefore, Maximus, Inc. should have implemented and maintained procedures and practices

appropriate to the nature and scope of information compromised in the Data Breach.

3264. As a result of Maximus, Inc.'s violation of PIPA, Plaintiff Plotke and the Illinois Maximus, Inc. Class Members incurred economic damages, including expenses associated with necessary credit monitoring.

MAXIMUS BELLWETHER COUNT XVI
VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT ("ICFA"), 815 ILCS 505/1, *et seq.*
(Brought on behalf of the Illinois Maximus, Inc. Class)

3265. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3266. Plaintiff Plotke brings this claim against Maximus, Inc. on behalf of the Illinois Maximus, Inc. Class.

3267. Section 2 of ICFA prohibits unfair or deceptive acts or practices and states, in relevant part, as follows:

> Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of such material fact, or the use or employment of any practice described in section 2 of the "Uniform Deceptive Trade Practices Act", approved August 5, 1965, in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby.

3268. Maximus, Inc. violated Section 2 of ICFA by engaging in unfair acts in the course of conduct involving trade or commerce when dealing with Plaintiff Plotke. Specifically, it was an unfair act and practice for Maximus, Inc. to represent to the public that it implemented commercially reasonable measures to protect Plaintiff Plotke's PII when it knew or should have known that it failed to fulfill such representations, including by preventing and failing to timely detect the Data Breach.

3269. Despite representing to Plaintiff Plotke and the Illinois Maximus, Inc. Class Members that it would implement commercially reasonable measures to protect their PII, Maximus, Inc. nonetheless failed to fulfill such representations.

3270. Plaintiff Plotke and the Illinois Maximus, Inc. Class Members have suffered injury in fact and actual damages, as alleged herein, as a result of Maximus, Inc.'s unlawful conduct and violations of the ICFA and analogous state statutes.

3271. Maximus, Inc.'s conduct offends public policy as it demonstrates a practice of unfair and deceptive business practices in failing to safeguard consumers' PII.

3272. An award of punitive damages is appropriate because Maximus, Inc.'s conduct described above was outrageous, willful and wanton, showed a reckless disregard for the rights of Plaintiff Plotke and consumers, generally, and Plaintiff Plotke had no choice but to submit to Maximus, Inc.'s illegal conduct.

MAXIMUS BELLWETHER COUNT XVII
VIOLATION OF THE ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT, 815 ILL. COMP. STAT. §§ 510/2, *et seq*.
(Brought on behalf of the Illinois Maximus, Inc. Class)

3273. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3274. Plaintiff Plotke brings this claim against Maximus, Inc. on behalf of the Illinois Maximus, Inc. Class.

3275. Maximus, Inc. is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

3276. Maximus, Inc. engaged in deceptive trade practices in the conduct of its businesses, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including, but not limited to:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

3277. Maximus, Inc.'s deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Plotke's PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Plotke's PII, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Plotke's PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Plotke's PII;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Plotke's PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Plotke's PII, including duties imposed by the FTCA, 15 U.S.C. § 45, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

3278. Maximus, Inc.'s representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' PII.

3279. The above unfair and deceptive practices and acts by Maximus, Inc. were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff Plotke

and the Illinois Maximus, Inc. Class that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

3280. As a direct and proximate result of Maximus, Inc.'s unfair, unlawful, and deceptive trade practices, Plaintiff Plotke and the Illinois Maximus, Inc. Class Members have suffered and will continue to suffer injury.

3281. Plaintiff Plotke and the Illinois Maximus, Inc. Class Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees and costs.

MAXIMUS BELLWETHER EIGHTEENTH CLAIM FOR RELIEF
VIOLATIONS OF THE Virginia Consumer Protection Act
Va. Code. Ann. §§ 59.1-196, *et seq*.
(Brought on behalf of the Maximus Nationwide Classes or, alternatively, the Maximus State Classes)

3282. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3283. Maximus Bellwether Plaintiffs bring this claim against Maximus on behalf of the Maximus Nationwide Classes or, alternatively, the Maximus State Classes (collectively, the Maximus Class").

3284. The Virginia Consumer Protection Act ("VACPA") is "applied as remedial legation to promote fair and ethical standards of dealings between suppliers and the consumer public." V.S. § 59.1-197. The VACPA prohibits "fraudulent acts or practices committed by a suppliers in connection with a consumer transaction[,]" including: "[m]isrepresenting that goods or services are of a particular standard, quality, grade, style, or model. *Id.* at § 59.1-200(6).

3285. Maximus engaged in deceptive acts or practices in violation of the VACPA. Specifically, Maximus performed the following:

a. Implementing and maintaining cybersecurity and privacy measures that were knowingly insufficient to protect Maximus Bellwether Plaintiffs' and the Maximus Class's sensitive data, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Maximus Bellwether Plaintiffs' and the Maximus Class's sensitive data, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Maximus Bellwether Plaintiffs' and the Maximus Class's sensitive data; and

e. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Maximus Bellwether Plaintiffs' and the Maximus Class's sensitive data, including duties imposed by the FTCA, 15 U.S.C. § 45. 191. Maximus is a "supplier" because it is a "seller . . . who advertises, solicits, or engages in consumer transactions . . . ." *Id.* at § 59.1-198.

3286. Maximus' omissions were material to Maximus Bellwether Plaintiffs and members of the Maximus Class because they were likely to and did deceive reasonable consumers about the adequacy of Maximus' data security and ability to protect the confidentiality of consumers' sensitive information that Maximus solicited, collected, and stored.

3287. Had Maximus disclosed to Maximus Bellwether Plaintiffs and the Maximus Class that its cybersecurity, digital platforms, and data storage systems were not secure and, thus, vulnerable to attack, Maximus would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law.

3288. Instead, Maximus received, maintained, and compiled Maximus Bellwether Plaintiffs' and the Maximus Class's sensitive data as part of the services Maximus provided and for which Maximus Bellwether Plaintiffs and members of the Maximus Class paid, in part, through

transaction fees by (1) omitting and concealing information from Maximus Bellwether Plaintiffs and the Maximus Class that Maximus' data security practices were knowingly insufficient to maintain the safety and confidentiality of Maximus Bellwether Plaintiffs' and the Maximus Class's sensitive data and (2) that Maximus was not compliant with basic data security requirements and best practices to prevent a data breach. Accordingly, Maximus Bellwether Plaintiffs and members of the Maximus Class acted reasonably in relying on Maximus' omissions, the truth of which they could not have discovered.

3289. Maximus Bellwether Plaintiffs and members of the Maximus Class seek all monetary and nonmonetary relief allowed by law, including statutory damages, actual damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the VCPA.

MAXIMUS BELLWETHER NINETEENTH CLAIM FOR RELIEF
Violations Of Virginia's Data Breach Notification Law
Va. Code. Ann. §§ 18.2-186.6, *et seq*.
(Brought on behalf of the Maximus Nationwide Classes or, alternatively, the Maximus State Classes)

3290. Maximus Bellwether Plaintiffs reallege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Five.

3291. Maximus Bellwether Plaintiffs bring this claim against Maximus on behalf of the Maximus Nationwide Classes or, alternatively, the Maximus State Classes (collectively, the Maximus Class).

3292. Maximus is required to accurately notify Maximus Bellwether Plaintiffs and the Maximus Class following discovery or notification of a breach of their data security system if decrypted or unredacted PII was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or

another fraud, without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

3293. Maximus is an entity that owns, licenses, or maintains computerized data that includes PII as defined by Va. Code Ann. §§ 18.2-186.6(B), (D).

3294. Maximus Bellwether Plaintiffs' and the Maximus Class's PII includes PII as covered under Va. Code Ann. § 18.2-186.6(A), including their names in conjunction with their Social Security numbers.

3295. Because Maximus discovered a breach of its security system in which decrypted or unredacted PII was or is reasonably believed to have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identify theft or another fraud, Maximus had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Va. Code Ann. §§ 18.2-186.6(B), (D). Yet Maximus waited over a month before notifying Maximus Bellwether Plaintiffs and members of the Maximus Class of the Data Breach.

3296. By failing to disclose the Data Breach in a timely and accurate manner, Maximus violated Va. Code Ann. §§ 18.2-186.6(B), (D).

3297. As a direct and proximate result of Maximus' violations of Va. Code Ann. §§ 18.2-186.6(B), (D), Maximus Bellwether Plaintiffs and members of the Maximus Class suffered damages, as described above.

3298. Maximus Plaintiffs and members of the Maximus Class seek relief under Va. Code Ann. § 18.2- 186.6(I), including actual damages.

VI. PRAYER FOR RELIEF AS AGAINST MAXIMUS

3299. Plaintiffs, individually and on behalf of the Maximus Bellwether Class, respectfully request that the Court grant the following relief:

a. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiffs as Class Representative and undersigned counsel as Class Counsel;

b. Find in favor of Plaintiffs and the Classes on all counts asserted herein;

c. Award Plaintiffs and the Classes actual, statutory, and/or punitive monetary damages to the maximum extent as allowed by law;

d. Award Plaintiffs and the Classes compensatory, consequential, general, and/or nominal monetary damages in an amount to be proven at trial;

e. Award Plaintiffs and the Classes restitution and all other applicable forms of equitable monetary relief;

f. Award Plaintiffs and the Classes equitable relief by enjoining Maximus from engaging in the wrongful conduct complained of herein regarding the misuse or disclosure of the private information of Plaintiffs and Class Members, and by requiring Maximus to issue prompt, complete, and accurate disclosure to Plaintiffs and Class Members;

g. Award Plaintiffs and the Classes injunctive relief as permitted by law or equity to assure that they have an effective remedy, and to protect the interests of Plaintiffs and Class Members, including, but not limited to, an order:

i. requiring Maximus to protect from unauthorized disclosure all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws, including by adequate encryption of all such data and by preventing unauthorized access to decryption keys;

ii. requiring Maximus to delete, destroy, and purge any personal identifying information of Plaintiffs and Class Members in its possession unless Maximus can provide to the Court reasonable justification for the retention and use of such information when weighted against the privacy interests of Plaintiffs and Class Members;

iii. requiring Maximus to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Maximus's systems on a periodic basis, and ordering Maximus to promptly correct any problems or issues detected by such third-party security auditors;

iv. requiring Maximus to engage independent third-party security auditors and internal personnel to run automated security monitoring including, but not limited to, regular database scanning and securing checks;

v. requiring Maximus to audit, test, and train its security personnel regarding any new or modified procedures;

vi. requiring Maximus to segment data by, among other things, creating firewalls and access controls so that if one area of Maximus network is compromised, hackers cannot gain access to other portions of Maximus's systems;

vii. requiring Maximus to establish for all Maximus employees an information security training program that includes annual training, with additional training to be provided as appropriate;

viii. requiring Maximus to establish for all Maximus security personnel a security training program that includes regularly scheduled internal training and education to inform Maximus's internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

ix. requiring Maximus to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Maximus's policies, programs, and systems for protecting personal identifying information;

x. requiring Maximus to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Maximus's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xi. requiring Maximus to provide notice to Plaintiffs and all Class Members regarding the full nature and extent of the Data Breach and the disclosure of Private Information to unauthorized persons, including the threat posed as a result of the disclosure of their confidential personal information, and educating Plaintiffs and Class Members regarding steps affected individuals should take to protect themselves;

xii. requiring Maximus to implement logging and monitoring programs sufficient to track traffic to and from Maximus's servers;

xiii. requiring, for a period of 10 years, the appointment of a qualified and independent third-party assessor to conduct an annual SOC 2 Type 2 attestation to evaluate Maximus's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Classes, and to report any deficiencies with compliance of the Court's final judgment;

xiv. requiring Maximus to implement multi-factor authentication requirements, if not already implemented; and

xv. requiring Maximus employees to employ passwords consistent with best security practices and to change their passwords on a timely and regular basis..

h. Award disgorgement and restitution of all earnings, profits, compensation, and benefits received by Maximus as a result of its unlawful acts;

i. Order Maximus to purchase or provide funds for lifetime credit monitoring and identify theft insurance to Plaintiffs and Class Members;

j. Order Maximus to pay all costs necessary to notice Class Members about the judgment and all costs necessary to administer a court approved claims process.

k. Award Plaintiffs and the Classes pre-judgment and post-judgment interest to the maximum extent allowed by law;

l. Grant Plaintiffs and the Classes leave to amend this complaint to conform to the evidence produced during the course of this case;

m. Award Plaintiffs and the Classes reasonable attorneys' fees, costs, and expenses, as allowable;

n. Where necessary, distribute any monies recovered from Maximus on behalf of Class Members or the general public via fluid recovery or cy pres recovery as applicable to prevent Maximus from retaining benefits of its wrongful conduct;

o. Award Plaintiffs and the Class such other favorable relief as allowable under law or at equity;

p. Award any other and further relief as may be just and proper; and

q. Conduct a trial by jury on all issues so triable.

CHAPTER SIX:

FACTUAL ALLEGATIONS AND CAUSES OF ACTION AGAINST WELLTOK

The Welltok Bellwether Plaintiffs (relisted for ease of review) Tamara Williams, Jeffrey Weaver, Amanda Copans, Denise Meyer, Christopher Rehm, Sherrie Rodda, Laquesha George, and Megan McClendon, individually and on behalf of all others similar situated, upon personal knowledge of facts pertaining to themselves, allege as follows against the Welltok Bellwether Defendants (relisted for ease of review) Welltok, Baylor Scott, Corewell, Sutter Health, OSF, CHI, and Virginia Mason.

I. Nature of Welltok's Business

3300. Welltok is a data-driven SaaS company that provides a consumer activation platform for the healthcare industry. Welltok's platform allows health plans, employers, healthcare providers, and public entities to connect with their consumers with personalized health improvement resources.[783]

3301. A consumer activation platform helps health plans, employers, healthcare providers, and public entities to incentivize consumer actions, such as getting a vaccine, scheduling a doctor's appointment, or selecting health insurance coverage. To incentivize consumer actions, an activation platform uses large datasets of consumer data, predictive analytics, and multi-channel communications to engage with consumers in a personalized manner.[784]

3302. Using Welltok Bellwether Plaintiffs' and Class Members' data provided by Welltok Clients, Welltok "can predict with up to 90% accuracy people's needs and their likelihood

[783] *See Welltok*, https://www.welltok.com/ (last accessed Nov. 6, 2024).

[784] *What is a Consumer Activation Platform?*, Personify Health, https://personifyhealth.com/resources/what-is-a-consumer-activation-platform/#:~:text=Healthcare%20marketing,selecting%20insurance%20coverage%20and%20more (last visited Nov. 6, 2024).

to take action, and engage them with integrated multi-channel outreach to maximise [sic] results."[785]

3303. Welltok's activation platform focuses "on motivating consumers, employees, patients, and members to complete targeted actions like participating in a mental health programme [sic], refilling a medication, or closing a gap in care." Put differently, Welltok's platform delivers digital and live solutions that engage consumers in "cultivating daily habits that improve outcomes across all aspects of their health and wellbeing." [786]

3304. Welltok's platform thus targets consumers at the individual level "by combining social determinants of health data with robust predictive analytics capabilities while leveraging multiple communication channels (text/SMS, email, interactive voice response (IVR) calls, social media, etc.)." By delivering personalized content and resources, Welltok motivates consumers to "take critical actions like scheduling an annual check-up, selecting insurance coverage or refilling medications."[787]

3305. Virgin Pulse acquired Welltok in 2021 in order to create an end-to-end engagement and activation platform for consumers across the healthcare industry. The engagement and activation platform would support consumers by:

a. Leveraging a comprehensive consumer data base of 275 million individuals and predictive analytics models to help Welltok Clients "generate social determinants of health insights to proactively address and reduce health disparities and close care gaps across" across their consumer populations;

---

[785] Virgin Pulse completes acquisition of Welltok, expanding health engagement capabilities for employers, payers and health systems, Virgin Pulse (Nov. 10, 2021), https://international.virginpulse.com/press-releases/virgin-pulse-completes-acquisition-of-welltok-expanding-health-engagement-capabilities-for-employers-payers-and-health-systems/.

[786] *Id.*

[787] *Id.*

b. Delivering health solutions that "engage users in improving their health and wellbeing every day"; and

c. Targeting activation across individuals to incentivize them to make tangible health outcomes through outreach and incentives.[788]

3306. As part of providing this activation platform and related services to Welltok Clients, Welltok uses MOVEit Transfer for transferring large datasets, including the transfer of Welltok Bellwether Plaintiffs' and Class Members' Private Information, via Welltok's MOVEit server.

A. Welltok Bellwether Defendants knew they were collecting sensitive information.

3307. Welltok and entities who contracted with Welltok, including the Welltok VCE Defendants, knew they needed to protect Welltok Bellwether Plaintiffs' and Class Members' Private Information.

3308. At all relevant times, Welltok Bellwether Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Welltok Bellwether Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Welltok's data security systems were breached, including, specifically, the significant costs that would be imposed on Welltok Bellwether Plaintiffs and Class Members as a result of a breach.

3309. As a condition to obtaining healthcare services, health plan services, and/or employment from Welltok VCE Defendants and other Welltok Clients, Welltok Bellwether Plaintiffs and Class Members were required to give their sensitive and confidential Private Information, either directly or indirectly, to Welltok VCE Defendants and Welltok Clients who contracted with Welltok. This information included, at a minimum, Welltok Bellwether Plaintiffs'

[788] *Id.*

and Class Members' names, dates of birth, addresses, health information, Social Security Numbers, Medicare / Medicaid IDs, and health insurance information.

3310. Unbeknownst to Welltok Bellwether Plaintiffs and Class Members, Welltok VCE Defendants, and Welltok Clients in turn, provided Welltok with access to that Private Information, directly or indirectly, to collect, store, and transfer using Welltok's platform that utilized MOVEit Transfer.

3311. For example, Sutter Health collected, stored, and transferred Welltok Bellwether Plaintiffs Meyer's and Copans's and other Class Members' Private Information in connection with healthcare services provided to them by Sutter Health. Sutter Health provided Welltok with access to Welltok Bellwether Plaintiffs Meyer's and Copans's and Class Members' Private Information by causing that information to be used, stored, and transferred to Welltok's activation platform, which utilized the MOVEit Transfer tool. According to the Data Breach Notice Letters that Welltok Bellwether Plaintiffs Meyer and Copans received from Welltok, "Welltok operates an online contact-management platform that enables healthcare clients to provide patients and members with important notices and communications for Sutter Health and received your information in connection with those services." The Private Information Sutter Health collected, stored, and transferred to Welltok included individuals' names, dates of birth, health insurance information, provider names, treatment cost information, and treatment information or diagnoses. Upon information and belief, this Private Information was transferred to Welltok via MOVEit Transfer and Welltok's MOVEit server.

3312. Similarly, OSF collected, stored, and transferred Welltok Bellwether Plaintiff Rehm's and other Class Members' Private Information in connection with healthcare services provided to them by OSF. OSF provided Welltok with access to Welltok Bellwether Plaintiff

Rehm's and Class Members' Private Information by causing that information to be used, stored, and transferred to Welltok's activation platform, which utilized the MOVEit Transfer tool. According to the Data Breach Letter Welltok Bellwether Plaintiff Rehm received from Welltok, "Welltok operates a member notification and contact platform for OSF Healthcare and received your information in connection with these services." The Private Information OSF collected, stored, and transferred to Welltok included individuals' dates of birth, Social Security Numbers, treatment information and diagnoses, provider names, MRN / patient IDs, health insurance information, and treatment cost information. Upon information and belief, this Private Information was transferred to Welltok via MOVEit Transfer and Welltok's MOVEit server.

3313. Similarly, Corewell collected, stored, and transferred Welltok Bellwether Plaintiffs Williams's and Weaver's and other Class Members' Private Information in connection with healthcare services provided to them by Corewell. Corewell provided Welltok with access to Welltok Bellwether Plaintiffs Williams's and Weaver's and Class Members' Private Information by causing that information to be used, stored, and transferred to Welltok's activation platform, which utilized the MOVEit Transfer tool. According to the Data Breach Letter Welltok Bellwether Plaintiffs Williams and Weaver received from Welltok, "Welltok software operates a contact platform for [Corewell] and received your information in connection with these services." The Private Information that Corewell collected, stored, and transferred to Welltok included individuals' names, dates of birth, email addresses, phone numbers, medical diagnoses, health insurance information, and Social Security Numbers. Upon information and belief, this Private Information was transferred to Welltok via MOVEit Transfer and Welltok's MOVEit server.

3314. Similarly, CHI collected, stored, and transferred Welltok Bellwether Plaintiff George's and other Class Members' Private Information in connection with healthcare services

provided to them by CHI. CHI provided Welltok with access to Welltok Bellwether Plaintiff George's and Class Members' Private Information by causing that information to be used, stored, and transferred to Welltok's activation platform, which utilized the MOVEit Transfer tool. According to the Data Breach Letter Welltok Bellwether Plaintiff George received from Welltok, "Welltok operates an online contact-management platform that enables healthcare clients to provide patients and members with important notices and communications for CHI Health - NE and received your information in connection with these services." The Private Information CHI collected, stored, and transferred to Welltok included individuals' names, addresses, dates of birth, clinical information, patient IDs, and health insurance information. Upon information and belief, this Private Information was transferred to Welltok via MOVEit Transfer and Welltok's MOVEit server.

3315. Similarly, Virginia Mason collected, stored, and transferred Welltok Bellwether Plaintiff McClendon's and other Class Members' Private Information in connection with healthcare services provided to them by Virginia Mason. Virginia Mason provided Welltok with access to Welltok Bellwether Plaintiff McClendon's and Class Members' Private Information by causing that information to be used, stored, and transferred to Welltok's activation platform, which utilized the MOVEit Transfer tool. According to the Data Breach Letter Welltok Bellwether Plaintiff McClendon received from Welltok, "Welltok operates an online contact-management platform that enables healthcare clients to provide patients and members with important notices and communications for Virginia Mason Franciscan Health and received your information in connection with these services." The Private Information Virginia Mason collected, stored, and transferred to Welltok included individuals' names, addresses, dates of birth, clinical information,

patient IDs, and health insurance information. Upon information and belief, this Private Information was transferred to Welltok via MOVEit Transfer and Welltok's MOVEit server.

3316. Similarly, Baylor Scott collected, stored and transferred Welltok Bellwether Plaintiff Rodda's and other Class Members' Private Information in connection with healthcare services provided to them by Baylor Scott. Baylor Scott provided Welltok with access to Welltok Bellwether Plaintiff Rodda's and Class Members' Private Information by causing that information to be used, stored, and transferred to Welltok's activation platform, which utilized the MOVEit Transfer tool. According to the Data Breach Letter Plaintiff Rodda received from Welltok, "Welltok operates an online contract-management platform that enables its healthcare clients, including Baylor Scott & White Health, to provide patients and members with important notices and communications, and received your information in connection with these services." The Private Information Baylor Scott collected, stored, and transferred to Welltok included individuals' names, Social Security numbers, date of birth, health insurance information, MRN/patient ID, provider name, treatment cost information, and treatment information/diagnosis. Upon information and belief, this Private Information was transferred to Welltok via MOVEit Transfer and Welltok's MOVEit server.

3317. Upon information and belief, other Welltok Clients who contracted with Welltok collected, stored, and transferred Class Members' Private Information in connection with healthcare or health plan services provided to them by other Welltok Clients. These other Welltok Clients provided Welltok with access to Class Members' Private Information by causing that information to be used, stored, and transferred to Welltok's activation platform, which utilized the MOVEit Transfer tool. Upon information and belief, this Private Information was transferred to Welltok via MOVEit Transfer and Welltok's MOVEit server.

3318. By obtaining, collecting, storing, and sharing Welltok Bellwether Plaintiffs' and Class Members' Private Information, Welltok Bellwether Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

3319. Due to the nature of Welltok Bellwether Defendants' businesses, Welltok Bellwether Defendants would be unable to engage in their regular business activities without collecting and aggregating Private Information they know and understand to be sensitive and confidential.

3320. Welltok Bellwether Plaintiffs and Class Members relied on Welltok Bellwether Defendants to implement and maintain adequate data security policies and protocols (including vetting, auditing, and monitoring vendors and software companies on which they relied) to keep their Private Information confidential and securely maintained, to use such Private Information (if at all) solely for business and healthcare purposes, and to prevent unauthorized access and disclosure of Private Information to unauthorized persons. Welltok Bellwether Plaintiffs and Class Members reasonably expected Welltok Bellwether Defendants would safeguard their highly sensitive information and keep that Private Information confidential.

3321. Welltok Bellwether Plaintiffs' reliance on Welltok Bellwether Defendants was reasonable, as all Welltok Bellwether Defendants made explicit promises to Welltok Bellwether Plaintiffs and Class Members to maintain and protect their Private Information. This further demonstrates Welltok Bellwether Defendants' understanding of the importance of securing Private Information. Notably, in their respective Privacy Notices and Privacy Policies, Welltok Bellwether Defendants claim that the privacy of individuals' Private Information is a top priority and pledge

a commitment to protecting that information from unauthorized use, including by using state-of-the-art care and the latest technologies to ensure the utmost security in doing so.

1. Welltok knew it was collecting, storing, and was responsible for protecting sensitive Private Information.

3322. For example, Welltok's parent Virgin Pulse pledges in its General Privacy Notice that "[w]e are committed to protecting your rights and your privacy. To ensure data security, We follow reasonable physical, electronic and managerial procedures designed to safeguard and secure your data and Personal Information." With respect to the transfer of its healthcare clients' and patients' personal information to authorized parties, Virgin Pulse represents that "[w]hen we receive Personal Information from a third party, or share Personal Information with a third party, we execute appropriate written agreements based on the applicable jurisdiction." Virgin Pulse's Privacy Notice "applies to all Personal Information whether collected online or offline" and warns users that "if you choose to withhold some Personal Information, We may be unable to provide you with certain services."[789]

3323. According to its Privacy Notice, Virgin Pulse collects, stores, and transfers "any information, including personal and material circumstances, that allows a person to become identifiable[,]" including, but not limited to:

a. Your email address;
b. Your profile information, including your profile photo;
c. Your gender, date of birth and age;
d. Your social security number or employee identification number;
e. Biometric information such as your blood pressure or weight;
f. Information about your health;
g. Information about your fitness and related wellness activities offered within the Program;
h. Information about your participation and performance in the Program and related challenges;

[789] *Terms of Use*, Personify Health, https://personifyhealth.com/terms-of-use/ (last updated Nov. 6, 2024).

i. Information you voluntarily share about yourself during any calls you participate in with Our health coaches;
j. Information you voluntarily share with Our Member Services team;
k. The comments and contributions you may make on the web-based platform or mobile application; and
l. Additional information you may provide as you submit queries and requests to Us.

3324. In addition, on its website, Virgin Pulse maintains an "Authorization For Use and Disclosure of Protected Health Information" (the "Authorization"), which "pertains to your right to the privacy of your Protected Health Information (PHI)."[790] The Authorization promises that:

> Your PHI, including health screening results, health assessment responses and coaching notes, will not be obtained by your Program Sponsor except as described in this Authorization and will not be used by your Program Sponsor for any employment-related purposes. Your PHI will not be sold, exchanged, transferred or otherwise disclosed to third parties for commercial purposes. Your PHI will not be disclosed except as permitted by this Authorization or Our Privacy Notice, or to the extent permitted by law. You will not be asked or required to waive the confidentiality of your PHI as a condition of participating in Our Program or receiving an incentive. You may not be discriminated against in employment because of the PHI you provide as part of participating in the wellness program, nor may you be subjected to retaliation if you choose not to participate.
>
> We will only share your PHI with entities that have a legal right to access it, that are obligated to protect it in similar ways that we are obligated to protect it, and that assist in providing Our Program or other health benefits to you…

3325. Welltok's General Privacy Notice (effective September 30, 2020), claims that "[p]rotecting your personal data is important to Welltok and its subsidiaries." Welltok's LinkedIn page also represents that its software platform is a "single, secure platform."[791]

3326. According to its Privacy Notice, Welltok obtains PII and PHI as follows:

---

[790] *Authorization For Use and Disclosure of the Protected Health Information*, Virgin Pulse (Dec. 1, 2023), https://www.virginpulse.com/gina-phi-notice/.

[791] LinkedIn, https://www.linkedin.com/company/welltok-inc-/ (emphasis added) (last visited Nov. 6, 2024).

> When you use any of our websites or mobile applications (the "Platform") or use our and our engagement/customer relationship management platforms and services ("CRM"), we may collect information about you, including information that can be used to identify you ("Personal Information").
>
> Additionally, we may collect Personal Information from your health plan, your employer's self-funded health plan, your employer, a health service provider, your pharmacy and/or other similar types of entities (your "Sponsor") or from other third parties described in this Privacy Notice.

3327. According to its Privacy Notice, the type of Private Information that Welltok collects, stores, and transfers includes, but is not limited to:

a. Social Security number;
b. Name;
c. Date of birth;
d. Email address;
e. Home address;
f. Business address;
g. Phone number;
h. Other identification numbers (e.g. state-issued identification number, member number, or employee number);
i. Geolocation Data; and
j. Biometric Information.[792]

3328. Welltok states that it "may also collect PHI as defined under the HIPAA, which is a regulated subset of Personal Information. Welltok explains "[w]e collect this data to provide you with the services and functionality that you request (the "Services"), as well as for the other purposes described in this Privacy Notice." Specific types of PHI collected by Welltok cited in its Privacy Notice include "claims information, lab and biometric information, electronic medical records/electronic health records, and program activity."[793] Additional types of Private Information specifically related to individuals' health that Welltok collects, stores, and transfers includes, but is not limited to:

---

[792] *Id.*

[793] *Id.*

a. Physical Activity and Movement Data;
b. Health Risk Assessments;
c. Lab Scores;
d. Data Related to Managed Health Programs;
e. Medications and Prescriptions;
f. Cognitive Assessment Data;
g. Health Conditions or Diseases;
h. Health Plan Information;
i. Insurance Information; and
j. Eating Habits and Nutrition.[794]

3329. Welltok's Policy Notice further promises, "[w]e may provide your PHI to a Sponsor, Connect Partner or third-party service provider as either a covered entity or a business associate. We will only disclose your PHI as allowed under HIPAA to provide you with the Services or with your express consent."[795]

3330. Welltok Bellwether Plaintiffs and Class Members relied on Welltok to implement and maintain adequate data security policies and protocols (including vetting, auditing, and monitoring vendors and software companies on which they relied) to keep their Private Information confidential and securely maintained, to use such Private Information (if at all) solely for business and healthcare purposes, and to prevent unauthorized access and disclosure of Private Information to unauthorized persons. Welltok Bellwether Plaintiffs and Class Members, by and through Welltok Clients, reasonably expected Welltok would safeguard their highly sensitive information and keep that Private Information confidential.

2. CHI knew it was collecting, storing, and was responsible for protecting sensitive Private Information.

3331. CHI collected, stored, and shared with Welltok, Welltok Bellwether Plaintiff George's and other Class Members' Private Information in connection with services provided to

[794] *Id.*

[795] *Id.*

them by CHI. Indeed, according to Welltok Bellwether Plaintiff George's Notice Letter, "Welltok operates an online contact-management platform that enables healthcare clients to provide patients and members with important notices and communications for CHI Health - NE and received your information in connection with these services."

3332. By obtaining, collecting, storing, and sharing Welltok Bellwether Plaintiff George's and Class Members' Private Information, CHI assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

3333. CHI made explicit promises to Welltok Bellwether Plaintiff George and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information. For example, CHI's Notice of Privacy Practices, which describes "how medical information about you may be used and disclosed and how you can get access to this information," makes the following pledge:

> We understand that your protected health information is private and personal. We are committed to protecting it. Hospitals, clinics, doctors, home health and hospice staff, and other staff members make a record each time you visit. This notice applies to all the records of your care at the facility, whether created by staff members or your doctor. [796]

3334. CHI's Notice further represents that, "[w]e will protect your protected health information as much as we can under the law. Sometimes state law gives more protection to your information than federal law. Sometimes federal law gives more protection than state law. In each case, we will apply the laws that protect your information the most."[797]

---

[796] *See Notice of Privacy Practices*, CHI Health (last updated Oct. 2020), https://www.chihealth.com/content/dam/chihealthcom/documents/patients-and-visitors/patient-notice-of-privacy-practices/privacy_english.pdf.

[797] *Id.*

3335. CHI assures members that CHI will not use or disclose their Private Information for any reasons not explicitly listed in the Notice (such as for medical treatment, health-care operations, research, and instances required by law) "unless we get your written permission. Under HIPAA, this permission is called an "authorization."[798]

3. Corewell knew it was collecting, storing, and was responsible for protecting sensitive Private Information.

3336. Corewell Health collected, stored, and shared with Welltok, Welltok Bellwether Plaintiffs Williams's and Weaver's and other Class Members' Private Information in connection with services provided to them by Corewell Health. Indeed, according to both Data Breach Notice Letters that Welltok Bellwether Plaintiffs Williams and Weaver received from Welltok, "Welltok software operates a contact platform for Corewell Health East and received your information in connection with those services."

3337. By obtaining, collecting, storing, and sharing Welltok Bellwether Plaintiffs Williams' and Weaver's and Class Members' Private Information, Corewell Health assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

3338. Corewell Health made explicit promises to Welltok Bellwether Plaintiff Williams and Weaver and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information. For example, Corewell Health's Notice of Privacy Practices, which all Corewell Health facilities are required to follow, asserts that "[w]e are committed to your privacy" and that "[t]he privacy of your health information has always been a priority at Corewell Health."[799] In that Notice, Corewell Health makes a "Pledge

[798] *Id.*

[799] *See* Notice of Privacy Practices (Patient Privacy) | Corewell Health (spectrumhealth.org)

Regarding Your Health Information," stating that "[w]e understand that your health information is personal, and we are committed to protecting it."[800] The Notice notes that Corewell Health's pledge to protect privacy rights is an "ongoing commitment."[801] According to the Notice, the information collected and stored by Corewell Health includes both physical and mental healthcare information.

3339. Corewell Health also maintains a Privacy Policy that "sets forth the guidelines used for protecting the information you … provide during visits to https://corewellhealth.org."[802] The type of information collected and stored by Corewell Health from patients and users includes their Private Information provided to participants in Corewell Health's healthcare network, the content of their email communications with Corewell Health, together with their email addresses and Corwell Health's responses thereto, and their website-use information as they browse Corewell Health's website.

3340. In the first paragraph of its Privacy Policy, Corewell Health promises that "[w]e will not sell, share, or rent this information to others in ways different from what is disclosed in this statement."[803] The ways disclosed in the Privacy Policy include "shar[ing] the information we collect with agents, contractors or affiliates of ours for the purpose of providing services to us."[804] The Privacy Policy also reserves the right to release collecting personal information when

[800] *Id.*

[801] *Id.*

[802] *Privacy Policy*, Corewell Health, https://corewellhealth.org/privacy-policy (last visited Nov. 6, 2024).

[803] *Id.*

[804] *Id.*

necessary to "comply with the law, other agreements, or to protect the rights, property, or safety of [https://corewellhealth.org], its owners or others."[805]

3341. Corewell Health also has a MyChart Privacy Policy concerning the Private Information collected and stored on Corewell Health's "MyChart" mobile application and website. In that Privacy Policy, Corewell Health states that "[t]he importance of security for all personal information including, but not limited to, health information associated with you, is of utmost concern to us. Through MyChart, we exercise state of the art care in providing secure transmission of your information from your computer or mobile device to our servers. Information collected by the MyChart site and app is stored in secure operation environments that are not available or accessible to the public."[806] Corewell Health further assures patients that "MyChart is not only HIPAA compliant but additionally utilizes the latest technologies to ensure utmost security."[807]

3342. The tools, features, and services available through MyChart include "access to your medical record information, (2) access to information in your Priority Health account (if you have one), and (3) connection to participating physicians and other licensed health care professionals ("Providers") in real time, via live video, telephone and/or secure email, for the diagnosis and treatment of patients over the Internet."[808] The MyChart Privacy Policy assures that Corewell Health "will not sell, share, or rent this information to others except: (i) when you've provided your prior consent; or (ii) as disclosed in this Policy."[809] The Private Information collected and

[805] *Id.*

[806] *Id.*

[807] *Id.*

[808] *Id.*

[809] *Id.*

stored by MyChart includes patients' medical records, the results of certain medical tests, claims summaries, as well as information that Corwell Health specifically requests from users when they:

a. Sign up for MyChart;
b. Provide preferred pharmacy locations;
c. Provide self-reported remedies, supplements and over-the-counter medications;
d. Provide self-reported immunizations;
e. Send a secure message to your health care provider, billing office or MyChart customer support;
f. Request an appointment or health service(s);
g. Access test results;
h. Connect and communicate with physicians or other licensed health care professionals ("Providers") in real time, via live streaming video, telephone and/or secure email for the purpose of diagnosis and/or treatment('eCareServices');
i. Use the Abriiz tool to record information about your health and wellness;
j. Request access or grant access to your account for another MyChart account user.

4. OSF knew it was collecting, storing, and was responsible for protecting sensitive Private Information.

3343. OSF collected, stored, and shared with Welltok, Welltok Bellwether Plaintiff Rehm's and other Class Members' Private Information in connection with services provided to them by OSF. Indeed, according to Welltok Bellwether Plaintiff Rehm's Notice Letter, "Welltok operates a member notification and contact platform for OSF Healthcare and received your information in connection with these services."

3344. By obtaining, collecting, storing, and sharing Welltok Bellwether Plaintiff Rehm's and Class Members' Private Information, OSF assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

3345. OSF made explicit promises to Welltok Bellwether Plaintiff Rehm and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information. For example, OSF's Privacy Notice acknowledges OSF's duty under federal law to "maintain the privacy of individually identifiable health

information."[810] Additionally, OSF's Patient Privacy & Rights represents "OSF HealthCare respects the privacy of our patients. Personal Privacy is very important to us. We work very hard to make sure the health information of our patients is properly protected.[811] OSF's Privacy Notice enumerates several ways OSF may use or disclose patients' PHI (such as for "treatment, payment, and health care operations") and patients' PII (such as to "facilitate your enrollment in the health plans and the provision and administration of your benefits").[812] The Notice assures patients that beyond the uses explicitly enumerated in the Notice, OSF "may not take any other uses and disclosures of your individually identifiable health information without your written authorization."[813]

5. Sutter Health knew it was collecting, storing, and was responsible for protecting sensitive Private Information.

3346. Sutter Health collected, stored, and shared with Welltok, Welltok Bellwether Plaintiffs Copans's and Meyer's and other Class Members' Private Information in connection with services provided to them by Sutter Health. Indeed, according to both Data Breach Notice Letters that Welltok Bellwether Plaintiffs Copans and Meyer received from Welltok, "Welltok operates an online contact-management platform that enables healthcare clients to provide patients and members with important notices and communications for Sutter Health and received your information in connection with those services."

---

[810] *Notice of Privacy Practices*, OSF Healthcare, https://osf-p-001.sitecorecontenthub.cloud/api/public/content/0035fe7bf4d343a6be0ef791363abe23?v=8ec04e19 (last updated Oct. 1, 2023).

[811] *Patient Privacy & Rights*, OSF Healthcare, https://x.osfhealthcare.org/patients-visitors/compliance/patient-privacy-rights (last visited Oct. 24, 2024).

[812] *Notice of Privacy Practices of the OSF Healthcare Single Affiliated Covered Entity*, OSF Healthcare (last updated Oct. 1, 2023), https://osf-p-001.sitecorecontenthub.cloud/api/public/content/0035fe7bf4d343a6be0ef791363abe23?v=8ec04e19.

[813] *Id.*

3347. By obtaining, collecting, storing, and sharing Welltok Bellwether Plaintiffs Copans's and Meyer's and Class Members' Private Information, Sutter Health assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

3348. Sutter Health made explicit promises to Welltok Bellwether Plaintiff Copans and Meyer and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information. For example, Sutter Health's Privacy Policy represents that "[p]rotecting your information is a top priority for Sutter. In addition to applying confidentiality policies that govern access and use of information by Sutter clinicians and staff, we have implemented physical, administrative, and technical security features and methods designed to safeguard your data in our information systems, including the use of, as appropriate, encryption, firewalls, monitoring, access controls, and other controls where appropriate."[814]

3349. Its Privacy Policy further states that Sutter Health and its affiliates collect certain information from individuals besides PHI "such as your name, address, phone number, email address, or other demographic information when you request additional information, search and apply for a job with Sutter, fill out a contact form, submit feedback to Sutter, attend a Sutter event, or otherwise engage with us. We may retain any messages you send us through the Sites pursuant to our retention policies. We use this information to operate, maintain, and provide you a superior website user experience as well as provide you information about Sutter."[815]

---

[814] *Privacy Policy*, Sutter Health (Aug. 1, 2024), https://www.sutterhealth.org/privacy/privacy-policy.

[815] *Id.*

3350. In its HIPAA and Privacy Practices, which apply to all healthcare providers in Sutter Health's network, Sutter Health acknowledges that it is "required by law to maintain the privacy and security of your protected health information. Sutter Health states that it can only use or share patients' PHI to treat them, run its organization (i.e.., managing patients' treatment and services), and bill and get payment from health plans, and in other ways that "contribute to the public good, such as public health and research," including to comply with the law, respond to organ and tissues requests, work with a medical examiner, and respond to workers' compensation, law enforcement, and other governmental requests.[816]

6. Virginia Mason knew it was collecting, storing, and was responsible for protecting sensitive Private Information.

3351. Virginia Mason collected, stored, and shared with Welltok, Welltok Bellwether Plaintiff McClendon's and other Class Members' Private Information in connection with services provided to them by Virginia Mason. Indeed, according to Welltok Bellwether Plaintiff McClendon's Notice Letter, "Welltok operates an online contact-management platform that enables healthcare clients to provide patients and members with important notices and communications for Virginia Mason Franciscan Health and received your information in connection with these services."

3352. By obtaining, collecting, storing, and sharing Welltok Bellwether Plaintiff McClendon's and Class Members' Private Information, Virginia Mason assumed legal and equitable duties and knew or should have known it was responsible for protecting the Private Information from disclosure.

[816] *HIPAA and Privacy Practices*, Sutter Health (June 12, 2017), https://www.sutterhealth.org/privacy/hipaa-privacy.

3353. Virginia Mason made explicit promises to Welltok Bellwether Plaintiff McClendon and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information. For example, Virginia Mason's Notice of Privacy Practices, which describes "how medical information about you may be used and disclosed and how you can get access to this information," makes the following pledge:

> We understand that your protected health information is private and personal. We are committed to protecting it. Hospitals, clinics, doctors, home health and hospice staff, and other staff members make a record each time you visit. This notice applies to all the records of your care at the facility, whether created by staff members or your doctor.[817]

3354. That Notice further represents that, "[w]e will protect your protected health information as much as we can under the law. Sometimes state law gives more protection to your information than federal law. Sometimes federal law gives more protection than state law. In each case, we will apply the laws that protect your information the most."[818]

3355. Virginia Mason assures members that it will not use or disclose their Private Information for any reasons not explicitly listed in the Notice (such as for medical treatment, health care operations, research, and instances required by law) "unless we get your written permission. Under HIPAA, this permission is called an 'authorization.'"[819]

7. Baylor Scott knew it was collecting, storing, and was responsible for protecting sensitive Private Information.

3356. Baylor Scott collected, stored, and collected, stored, and shared with Welltok, Welltok Bellwether Plaintiff Rodda's and other Class Members' Private Information in connection

---

[817] *Notice of Privacy Practices*, Virginia Mason Franciscan Health (June 2022), https://www.vmfh.org/content/dam/vmfhorg/pdf/vmfh-npp-english.pdf.

[818] *Id.*

[819] *Id.*

with services provided to them by Baylor Scott. Indeed, according to Welltok Bellwether Plaintiff Rodda's Notice Letter, "Welltok operates an online contact-management platform that enables its healthcare clients, including Baylor Scott & White Health, to provide patients and members with important notices and communications, and received your information in connection with these services."

3357. By obtaining, collecting, storing, and sharing Welltok Bellwether Plaintiff Rodda's and Class Members' Private Information, Baylor Scott assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

3358. Baylor Scott made explicit promises to Welltok Bellwether Plaintiff Rodda and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information. For example, Baylor Scott represents that it "values the privacy and health information of our visitors and patients."[820] Baylor Scott's Notice of Privacy Practices further acknowledges that Baylor Scott is "required by law to maintain the privacy and security of your protected health information."[821] The Notice also promises that "[w]e will let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[822]

---

[820] *Privacy Policies and Patient Rights*, Baylor Scott & White Health, https://www.bswhealth.com/privacy-policies-and-patient-rights (last visited Nov. 29, 2024).

[821] *Notice of Privacy Practices*, Baylor Scott & White (Oct. 2022), https://www.bswhealth.com/-/media/project/bsw/sites/bswhealth/documents/privacy-and-patient-rights/notice-of-privacy-practices.pdf?sc_lang=en&hash=A13A2DE5DAE030FD9AD61086C2D0F13B.

[822] *Id.*

3359. The Notice assures patients that Baylor Scott "will not use or share your information other than as described here."[823] The Notice enumerates the ways in which Baylor Scott shares patients' Private Information, including to treat patients, run Baylor Scott's organization, communicate with patients, bill patients for services, help with public health and safety issues, provide proof of immunization to schools, conduct health research, make disclosures to the FDA, and comply with the law.[824]

3360. None of Welltok Defendants' respective Privacy Notices or Privacy Policies permitted any Welltok Defendant to share or disclose Welltok Bellwether Plaintiffs' and Class Members' Private Information to unauthorized third parties as occurred in the Data Breach.

B. Welltok Bellwether Defendants knew the risks of collecting this sensitive information.

3361. Welltok was, or should have been, fully aware of the unique type and the significant volume of data on its networks, including more than fourteen million individuals' detailed Private Information, and therefore was or should have been aware of the significant number of individuals who would be harmed by the compromise and theft of their decrypted data.

3362. Similarly, Welltok VCE Defendants were, or should have been, fully aware of the unique type and the significant volume of data they collected from their patients, members, and consumers, and therefore were or should have been aware of the significant number of individuals who would be harmed by the compromise and theft of their decrypted data.

3363. Because of the highly sensitive and personal nature of the Private Information Welltok Bellwether Defendants solicit, acquire, store, and maintain with respect to patients, customers, and/or users and other individuals, Welltok Bellwether Defendants, upon information

[823] *Id.*

[824] *Id.*

and belief, promise to, among other things: keep Private Information private; comply with industry standards related to data security and Private Information, including FTC guidelines; inform consumers of their legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to the products and services Welltok Bellwether Plaintiffs and Class Members obtain from Welltok Bellwether Defendants; and provide adequate notice to individuals if their Private Information is disclosed without authorization. As sophisticated business entities handling highly sensitive and confidential consumer data, Welltok Bellwether Defendants' data security obligations were particularly important, especially in light of the substantial increase in cyberattacks and data breaches in industries handling significant amounts of Private Information preceding the date of the MOVEit Data Breach.

3364. At all relevant times, Welltok Bellwether Defendants knew, or should have known, that Welltok Bellwether Plaintiffs' and Class Members' Private Information was a target for malicious actors.

3365. Despite such knowledge, Welltok Bellwether Defendants implemented inadequate data privacy and security measures to that were insufficient to protect Welltok Bellwether Plaintiffs' and Class Members' Private Information from cyberattacks, including, but not limited to, inadequately vetting, auditing, monitoring, testing, and patching of the software applications they used to store and transfer such data and/or adequately vetting, auditing, or monitoring the applications and security protocols of vendors that Welltok Bellwether Defendants contracted with.

3366. In light of recent high profile data breaches—including breaches arising from previously exploited vulnerabilities in other file transfer applications (e.g., Accellion FTA, Fortra

GoAnywhere MFT)—Welltok Bellwether Defendants knew or should have known that their electronic records and consumers' Private Information would be targeted by cybercriminals and ransomware attack groups.

3367. "Third-party software security risks are on the rise, and so are the significant cyberattacks they facilitate. According to a CrowdStrike report, 45% of surveyed organizations said they experienced at least on software supply chain attack in 2021."[825] Indeed, a recent study found that the healthcare industry "was the worst affected industry with the highest volume of third-party breaches," with the vendors experiencing the most breaches being those that provided software, IT products, and related services.[826]

3368. Recent high profile cybersecurity incidents at healthcare partner and provider companies, including NextGen Healthcare, Inc. (1.5 million patients, April 2024), OneTouchPoint, Inc. (4.1 million patients, July 2022), Shields Healthcare Group (2 million patients, March 2022), Blackbaud, Inc. (millions of individuals, May 2020), American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), put Welltok Bellwether Defendants on notice that their electronic records would be targeted by cybercriminals.

---

[825] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard (last updated Sept. 4, 2023), https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software.

[826] Steve Alder, *Healthcare Experiences More Third-Party Data Breaches Than Any Other Sector*, (Mar. 4, 2024), https://www.hipaajournal.com/healthcare-highest-third-party-breaches/.

3369. Because of the value of the type of data the medical industry collects and stores, the medical industry is a prime target for threat actors and has experienced disproportionally higher numbers of data theft events than other industries. Between 2009 and 2023, 5,887 healthcare data breaches of 500 or more individuals have been reported to Health and Human Services' Office of Civil Rights. Those breaches have resulted in the exposure of 519,935,970 healthcare records, a number that equates to 1.5x the population of the United States.[827]

3370. According to the HIPAA Journal's 2023 Healthcare Data Breach Report, "[a]n unwanted record was set in 2023 with 725 large security breaches in healthcare reported to the Department of Health and Human Services Office for Civil Rights, beating the record of 720 healthcare security breaches set the previous year."[828]

3371. In light of recent high profile data breaches at other health care partner and provider companies, the Welltok Bellwether Defendants knew or should have known that their electronic records and consumers' Private Information would be targeted by cybercriminals and ransomware attack groups.

3372. The breadth of the data exfiltrated from Welltok's MOVEit server in the Data Breach makes the information particularly valuable to cybercriminals and identity thieves, leaving Welltok Bellwether Plaintiffs and Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

3373. Social Security numbers (such as those compromised in the Data Breach) are among the worst kinds of Private Information to have stolen because they may be put to a variety

---

[827] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/, (last visited Nov. 6, 2024).

[828] Steve Adler, *Security Breaches in Healthcare in 2023*, The HIPAA Journal (Jan. 31, 2024), https://www.hipaajournal.com/wp-content/uploads/2024/01/Security_Breaches_In_Healthcare_in_2023_by_The_HIPAA_Journal.pdf.

of fraudulent uses and are difficult for an individual to change. Indeed, unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique Social Security numbers cannot easily be replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

3374. The Social Security Administration stresses that the loss of an individual's Social Security number can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other Private Information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[829]

3375. The Social Security Administration also warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other Private Information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other Private Information, such as your name and address, remains the same.

[829] *Identity Theft and Your Social Security Number*, Social Security Administration (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[830]

3376. Social Security numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often Social Security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes Social Security numbers a prime target for cybercriminals and a particularly attractive form of Private Information to steal and then sell.

3377. Medical information (such as that compromised in the Data Breach) is also highly valuable to cybercriminals. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[831] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[832]

---

[830] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[831] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[832] *Managing Cyber Risks in an Interconnected World, Key Findings from the Global State of Information Security® Survey 2015*, PriceWaterhouseCoopers, https://www.pwc.com/gx/en/

3378. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[833]

3379. As highly sophisticated parties that handle sensitive Private Information, Welltok Bellwether Defendants failed to establish and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Welltok Bellwether Plaintiffs' and Class Members' Private Information.

3380. The ramifications of Welltok Bellwether Defendants' failures to keep Welltok Bellwether Plaintiffs' and Class Members' Private Information secure are severe and long-lasting. To avoid detection, identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the "dark web" may take months or more to reach end-users, in

---

consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[833] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

part because the data can be sold in small batches to multiple buyers as opposed to in bulk to a single buyer. Thus, Welltok Bellwether Plaintiffs and Class Members must vigilantly monitor their accounts, and Welltok Bellwether Plaintiffs and Class Members are at an increased risk of fraud and identity theft, for many years into the future.

3381. Thus, Welltok Bellwether Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to them and of the foreseeable consequences if their systems were breached. Welltok Bellwether Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring or from mitigating the consequences of the Data Breach.

C. Welltok Bellwether Defendants did not do enough to protect the data given the sensitivity of it, including properly vetting Progress's software and cybersecurity practices.

3382. Welltok Bellwether Defendants knew, or should have known, the importance of safeguarding the Private Information entrusted to them, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on affected individuals as a result of a data breach.

3383. Each Welltok Bellwether Defendant therefore owed a duty to Welltok Bellwether Plaintiffs and Class Members to implement and maintain reasonable and adequate data security measures to secure, protect, and safeguard the Private Information entrusted to them by Welltok Bellwether Plaintiffs and Class Members.

3384. Welltok Bellwether Defendants should have used their resources to implement and maintain adequate data security procedures and practices.

3385. Welltok Bellwether Defendants breached their duties to Welltok Bellwether Plaintiffs and Class Members by, among other things, failing to employ adequate vendor screening and vetting, including of Progress and its MOVEit Transfer application.

3386. Welltok Bellwether Defendants knew or should have known that Progress: employed poorly-written, outdated, and insecure code in its MOVEit Transfer application; failed to update outdated code; and failed to check for known or newly discovered vulnerabilities.

3387. Welltok and Welltok VCE Defendants who contracted with Welltok should have but did not vet Progress or its MOVEit Transfer application, and as a result, failed to prevent or detect the Data Breach.

3388. Welltok and Welltok VCE Defendants who contracted with Welltok failed to ensure Progress employed and maintained adequate cybersecurity measures to prevent the Data Breach from occurring.

3389. Welltok Bellwether Defendants also had obligations arising under the FTC Act, HIPAA, industry standards, common law, and their own promises and representations made to Welltok Bellwether Plaintiffs and Class Members to keep their Private Information confidential and protected from unauthorized access and disclosure.

1. Welltok Bellwether Defendants fail to comply with FTC guidelines.

3390. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

3391. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal consumer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer

networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[834]

3392. The FTC guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach.[835]

3393. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

3394. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

3395. Upon information and belief, Welltok Bellwether Defendants failed to properly implement the foregoing recommended data security practices.

3396. Welltok Bellwether Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to the Private Information in their care and failure

---

[834] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[835] *Id.*

to employ reasonable and appropriate oversight of vendors to whom they entrusted Private Information in their care constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

3397. Welltok Bellwether Defendants were at all times fully aware of their obligations to protect the Private Information entrusted to them. Welltok Bellwether Defendants were also aware of the significant repercussions that would result from their failure to do so.

2. Welltok Bellwether Defendants violated their HIPAA obligations.

3398. Because the Welltok Bellwether Defendants receive, maintain, and handle PHI, the Welltok Bellwether Defendants are either (1) healthcare service providers handling medical patient data and/or providing services to hospitals and healthcare organizations that are covered entities under HIPAA pursuant to 45 C.F.R. § 160.103, or (2) business associates of healthcare service providers pursuant to 45 C.F.R. § 160.103. As such, all Welltok Bellwether Defendants are covered entities required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C ("Security Standards for the Protection of Electronic Protected Health Information").

3399. HIPAA requires covered entities and business associates to protect against reasonably anticipated threats to the security of sensitive patient health information.

3400. Welltok Bellwether Defendants are also subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921; 45 C.F.R. § 160.103.

3401. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form.

3402. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

3403. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

3404. Under 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media," "[m]aintained in electronic media," or "[t]ransmitted or maintained in any other form or medium."

3405. Under 45 C.F.R. § 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual;" and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual."

3406. HIPAA required the Welltok Bellwether Defendants to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 C.F.R. § 164.102, *et seq*.

3407. HIPAA also requires covered entities and business associates to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, covered entities and business associates are required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

3408. HIPAA and HITECH also obligate covered entities and business associates to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. § 17902.

3409. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires covered entities and business associates to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 calendar days after discovery of a breach***." (emphasis added).

3410. The Data Breach, as it related to Welltok Bellwether Defendants, is considered a breach under the HIPAA Rules because it involved an access of PHI not permitted under the HIPAA Privacy Rule.

3411. A breach under the HIPAA Rules is defined as "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. § 164.40.

3412. The Data Breach resulted from a combination of insufficiencies that demonstrate Welltok Bellwether Defendants failed to comply with safeguards mandated by HIPAA regulations.

3413. As HIPAA covered entities, Welltok Bellwether Defendants are required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured PHI, as in the case of the Data Breach.

3414. As HIPAA-covered entities handling medical patient data, Welltok Bellwether Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the Data Breach.

3. Welltok Bellwether Defendants failed to comply with industry standards.

3415. Several best practices have been identified that at a minimum should be implemented by entities, like Welltok Bellwether Defendants, that handle highly sensitive and confidential Private Information.

3416. These best practices include, but are not limited to: educating all employees about data security practices and procedures; requiring strong passwords; implementing multi-layer security—including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; adequately securing encryption keys to prevent unauthorized access; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

3417. Other standard cybersecurity practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers;

monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

3418. On information and belief, Welltok Bellwether Defendants failed to meet the minimum standards of any of the following frameworks: the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

3419. On information and belief, Welltok Bellwether Defendants failed to meet Health and Human Services' recommendations that covered entities, such as the Welltok Bellwether Defendants, should implement to protect against some of the more common, and often successful, cyber-attack techniques:

a. Regulated entities should implement security awareness and training for all workforce members and that the training programs should be ongoing, and evolving to be flexible to educate the workforce on new and current cybersecurity treats and how to respond;

b. Regulated entities should implement technologies that examine and verify that received emails do not originate from known malicious site, scan web links or attachments included in emails for potential threats, and impeded or deny the introduction of malware that may attempt to access PHI;

c. Regulated entities should mitigate known data security vulnerabilities by patching or upgrading vulnerable technology infrastructure, by upgrading or replacing obsolete and/or unsupported applications and devices, or by implementing safeguards to mitigate known vulnerabilities until an upgrade or replacement can occur;

d. Regulated entities should implement security management processes to prevent, detect, contain, and correct security violations, including conducting risk assessments to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI; and

e. Regulated entities should implement strong cyber security practices by requiring strong passwords rules and multifactor identification.[836]

3420. These foregoing frameworks are existing and applicable industry standards, and Welltok Bellwether Defendants failed to comply with these accepted standards, thereby opening the door to CL0P and causing the Data Breach.

3421. Welltok Bellwether Defendants' unlawful conduct therefore includes, but is not limited to, the following acts and/or omissions:

a. Implementing inadequate data security system that did not adequately protect against the risk of data breaches and cyberattacks;

b. Inadequately protecting Welltok Bellwether Plaintiffs', clients', patients', and employees' Private Information;

c. Inadequately monitoring their own data security systems for existing intrusions;

d. Inadequately training their employees and vendors regarding the proper handling of Welltok Bellwether Plaintiffs', clients', patients', and employees' Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to HIPAA guidelines and industry standards for cybersecurity as discussed above; and,

g. Otherwise breaching their duties and obligations to protect Welltok Bellwether Plaintiff's and Class Members' Private Information.

3422. The Welltok Bellwether Defendants instituted inadequate security controls and/or failed to institute the security controls that would have prevent the Data Breach, including those above, and affirmatively mishandled the maintenance, storage, and transfer of the Private

[836] *OCR Quarter 1 2022 Cybersecurity Newsletter*, U.S Dep't. of Health & Human Services (last updated Mar. 17, 2022), https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-first-quarter-2022/index.html.

Information in which the Welltok Bellwether Defendants were entrusted, leading to the Data Breach.

3423. The Welltok Bellwether Defendants affirmatively breached their obligations and duties to Welltok Bellwether Plaintiffs and Class Members and/or were otherwise negligent because they mismanaged their data security systems, policies, and procedures, failing to adequately safeguarded Welltok Bellwether Plaintiffs' and Class Members' Private Information.

D. Welltok Bellwether Defendants didn't do enough to vet their vendors' practices, including Progress.

3424. Welltok Bellwether Defendants are responsible for protecting the Private Information they solicit, collect, acquire, and maintain from attacks and breaches that result from weaknesses in third-party systems and software.

3425. Welltok Bellwether Defendants failed to safeguard Welltok Bellwether Plaintiffs' and Class Members' Private Information when they failed to adopt and enforce reasonable and available data security practices and procedures to prevent and/or mitigate the known risk of a cyberattack.

3426. Prior to the Data Breach, Welltok Bellwether Defendants should have, but did not, implement and maintain reasonable and necessary data security policies and procedures, which would have mitigated or avoided the Data Breach.

3427. There are numerous known and available steps that Welltok Bellwether Defendants could have taken to mitigate or even prevent the Data Breach.

3428. Data security practices that could and should have been implemented by Welltok Bellwether Defendants to prevent the Data Breach include:

a. Auditing of third-party software, including the MOVEit Transfer software;

b. Vetting and periodic auditing of third-party vendors, including Progress and, in the case of Welltok VCE Defendants, Welltok;

c. Restricting MOVEit transfers to pre-approved IP addresses ("whitelisting");

d. Limiting the specific types of files that can be uploaded;

e. Conducting basic monitoring of web servers;

f. Using web application firewalls ("WAFs"); and

g. Employing supply chain security.

1. Auditing Third-Party Software

3429. Security audits of third-party software enable companies to identify vulnerabilities, monitor access to sensitive data, and discover and remediate any unauthorized data access.[837] Here, security auditing of the MOVEit Transfer software could have prevented the Data Breach. The methods for conducting security audits of third-party software are well-known and widely available.[838] Welltok Bellwether Defendants therefore could and should have employed companies that conduct security audits of third-party software.[839]

2. Vetting Vendors

3430. In addition to auditing third-party software, proper vetting and routine audits of vendors' data security practices, including vetting of Progress's cybersecurity practices or Welltok's cybersecurity practices, could have prevented the Data Breach. Vendor risk assessments or security questionnaires are "one of the best methods for extracting deep cybersecurity insights about any aspects of a vendor's attack surface."[840] Industry-standard risk assessments and security

[837] *6 Security Tips for Third Party* Software, Cybersecurity Insiders, https://www.cybersecurity-insiders.com/6-security-tips-for-third-party-software/ (last visited Nov. 6, 2024).

[838] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard, https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-software (updated Oct. 31, 2024).

[839] Davit Asatryan, *Third-Party Applications Audit: Complete Guide*, Spin.ai (Nov. 4, 2021, updated Apr. 19, 2024), https://spinbackup.com/blog/third-party-applications-audit/.

[840] Edward Kost, *Third-Party Risk Management: How to Identify Vulnerable Third-Party Software (Quickly)*, UpGuard, https://www.upguard.com/blog/how-to-identify-vulnerable-third-party-

questionnaires designed to help companies discover vulnerabilities in third-party web applications and software are widely available,[841] and can be used to assess the security of third-party software against common attack vectors, including SQL injection susceptibility.[842]

3. Whitelisting

3431. Restricting MOVEit transfers to pre-approved IP addresses—a cybersecurity practice referred to as "whitelisting"—could also have prevented the Data Breach. A whitelist is an administrator-defined register of entities pre-approved for authorized access or to perform specific actions. Whitelisting enhances the security of a system or network by ensuring that only pre-approved users or devices have access to sensitive data or systems. Whitelisting thus denies access by default, providing authorization only to a vetted, pre-approved list of IP addresses, applications, email addresses, and/or users. Blacklisting, in contrast, requires that known threats be specifically identified and blocked, while everything else is permitted. By definition, a blacklist cannot protect against an exploitation of a Zero-Day vulnerability, like the one CL0P exploited in the MOVEit Data Breach. NIST Special Publication 800-167: *Guide to Application Whitelisting* provides specific guidance to companies on how to implement whitelisting.[843]

4. Limiting Specific File Types

3432. Limiting the specific types of files that can be uploaded via FTP could also have prevented the Data Breach. After exploiting the MOVEit vulnerability via SQL injection, CL0P

---

software (updated Oct. 31, 2024) ("Risk assessments can either be framework-based to identify security control deficiencies against popular security standards or custom-designed for focused investigations about specific third-party risks.").

[841] *Id.*

[842] *Id.*

[843] Adam Sedgewick, Murugiah Souppaya, & Karen Scarfone, *Guide to Application Whiselisting*, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf (Oct. 2015).

uploaded the LEMURLOOT web shell, which masqueraded as a legitimate file[844] and allowed the threat actor to execute commands, download files, extract system settings, and create/insert/delete users.[845]

3433. Proper data security dictates that only those files that are needed and expected to be uploaded should be allowed. This typically includes document file types such as .doc, .docx, .pdf, etc. Only web site administrators with whitelisted IP addresses should have been allowed to upload web page files, such as .aspx.

5. Adequate Logging, Monitoring, and Auditing

3434. "Logging, monitoring, and auditing procedures help an organization prevent incidents and provide an effective response when they occur."[846] These tools can detect SQL injection attempts and mitigate or even prevent breaches like the MOVEit Data Breach.

3435. Forensic examinations of the MOVEit Data Breach have confirmed that indicators of compromise were found in the logs of targeted organizations,[847] verifying that effective log monitoring would have mitigated or even prevented the Data Breach. Accordingly, Welltok

[844] Kunal Modasiya, Progress MOVEit Transfer Vulnerability Being Actively Exploited Qualys (Aug. 7, 2023), https://blog.qualys.com/vulnerabilities-threat-research/2023/06/07/progress-moveit-transfer-vulnerability-being-actively-exploited; *see also* Jonathan Reed, The MOVEit breach impacted and fallout: How can you respond?, Security Intelligence (July 19, 2023), https://securityintelligence.com/news/the-moveit-breach-impact-and-fallout-how-can-you-respond/.

[845] *#StopRansomware: Cl0p Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, CISA (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[846] Mike Chapple, et al., (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide (9th ed. 2021).

[847] Scott Downie, et al., *Transfer Vulnerability (CVE-2023-34362) Since* 2021, Kroll (June 8, 2023), https://www.kroll.com/en/insights/publications/cyber/clop-ransomware-moveit-transfer-vulnerability-cve-2023-34362.

Bellwether Defendants could and should have utilized commonly available tools that monitor logs automatically and provide alerts of unusual activity to administrators.

3436. "Several different logs record details of activity on systems and networks. For example, firewall logs record details of all traffic that the firewall blocked. By monitoring these logs, it's possible to detect incidents. Some automated methods of log monitoring automatically detect potential incidents and report them right after they've occurred."[848]

3437. Here, adequate logging and log monitoring could have prevented the MOVEit Data Breach because logs would have shown clear indicators of compromise and/or malicious activity. SQL injection attempts, successful or not, will appear in such logs. But even extensive logging is insufficient without adequate monitoring of said logs.

3438. NIST publishes a Cybersecurity Framework that emphasizes continuous monitoring of systems.[849] The NIST SP 800-92 Guide to Computer Security Log Management further defines how to manage logs,[850] and there are a number of widely available tools that can monitor logs automatically and provide alerts to administrators when there is unusual activity.

3439. Monitoring web server logs for new files, as recommended in NIST SP 800-12,[851] is a widely accepted cybersecurity practice[852] that would have promptly detected the new files

[848] Darril Gibson, CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide at p. 73 (2017).

[849] NIST, *The NIST Cybersecurity Framework (CSF) 2*.0, Nat'l Inst. of Standards and Tech. (Feb. 26, 2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[850] NIST, *Guide to Computer Security Log Management*, Nat'l Inst. of Standards and Tech. (Sept. 2006), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf.

[851] NIST, *An Introduction to Information Security*, NIST Special Publication 800-12, Rev. 1 (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

[852] *Monitor web server directories for changed / new files*, https://serverfault.com/questions/1145284/monitor-web-server-directories-for-changed-new-files (last visited May 20, 2024);

introduced in the MOVEit Data Breach. Web server monitoring would have specifically allowed Welltok Bellwether Defendants to detect the new files introduced to the web server root (human.aspx and human2.aspx) that enabled CL0P to perpetrate the MOVEit Data Breach. Even basic monitoring of Welltok Bellwether Defendants' web servers could therefore have prevented the Data Breach because it would have revealed the backdoor CL0P introduced to the web server.[853]

3440. In addition to file system monitoring to identify new files, the InfoSec institute recommends: (a) network monitoring to identify rogue IP addresses which may be performing malicious activities such as brute-force or fuzzing; (b) authentication monitoring to identify unusual logins or login attempts; (c) file change monitoring to identify changes to sensitive files within the file system; and (d) process monitoring to identify rogue processes that might be malicious.[854]

3441. Beyond monitoring activity, the actual data transferred via MOVEit could and should have been monitored by Welltok Bellwether Defendants. Most legitimate interactions utilizing MOVEit only upload or download relatively small amounts of data at a given time, but CL0P was able to exfiltrate large amounts of consumer data in the Data Breach. Had Welltok Bellwether Defendants been adequately monitoring data transfers, any attempt to exfiltrate large amounts of data (significantly varying from normal usage) would have triggered an alert.

Gateway Script to monitor directory for new files, Ignition https://forum.inductiveautomation.com/t/gateway-script-to-monitor-directory-for-new-files/16124/5 (last visited Nov. 6, 2024).

[853] Tyler Lioi, *MOVEit Transfer Investigations*, CrowdStrike Blog (June 5, 2023), https://www.crowdstrike.com/blog/identifying-data-exfiltration-in-moveit-transfer-investigations/.

[854] Lester Obbayi, *Web server protection: Web server security monitoring*, InfoSec (May 4, 2020), https://www.infosecinstitute.com/resources/network-security-101/web-server-protection-web-server-security-monitoring/.

6. WAFs

3442. Properly configured web application firewalls ("WAFs") could also have prevented or mitigated the effects of the MOVEit Data Breach.[855]

7. Supply Chain Security

3443. Supply chain security is another common method of ensuring that all items in the supply chain, including third-party software like MOVEit, is secure.[856]

3444. NIST explicitly discusses vulnerabilities in third-party software and provides three supply chain security principles that, if applied, would have mitigated or prevented the MOVEit breaches:[857]

Figure 45

Cyber Supply Chain Security Principles:

1. **Develop your defenses based on the principle that your systems will be breached**. When one starts from the premise that a breach is inevitable, it changes the decision matrix on next steps. The question becomes not just how to prevent a breach, but how to mitigate an attacker's ability to exploit the information they have accessed and how to recover from the breach.
2. **Cybersecurity is never just a technology problem, it's a people, processes and knowledge problem**. Breaches tend to be less about a technology failure and more about human error. IT security systems won't secure critical information and intellectual property unless employees throughout the supply chain use secure cybersecurity practices.
3. **Security is Security.** There should be no gap between physical and cybersecurity. Sometimes the bad guys exploit lapses in physical security in order to launch a cyber attack. By the same token, an attacker looking for ways into a physical location might exploit cyber vulnerabilities to get access.

---

[855] *See, e.g.*, *Web Application Firewall*, Imperva, https://www.imperva.com/products/web-application-firewall-waf/ (last visited Nov. 6, 2024); Huawei Cloud, *How Does WAF Detect SQL Injection, XSS, and PHP Injection Attacks?* (Sept. 6, 2023), https://support.huaweicloud.com/intl/en-us/waf_faq/waf_01_0457.html.

[856] NIST, *Best Practices in Cyber Supply Chain Risk Management*, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf (last visited Nov. 6, 2024).

[857] *Id.*

8. Windows Security Feature

3445. Welltok Bellwether Defendants utilizing Windows have an additional protection modality. The Windows security system has ransomware protection, which allows the user to designate any folder as protected. Any attempt to add new files or change existing files in that folder would then have to be approved. Because LEMURLOOT masqueraded as a legitimate file that was then used as a backdoor, having the folder \inetpub\wwwroot\ protected from alterations would have prevented these files from being uploaded.

3446. In addition to the foregoing data security practices, which, if adopted by Welltok Bellwether Defendants, could have prevented the Data Breach, there are a number of common security techniques and mechanisms that should be a part of any standard data security policy and could have limited the scope of damage from a data breach. These security techniques and practices include:

a. Limiting access by employing a "least privileges" policy;

b. Implementing "zero-trust" security frameworks;

c. Encrypting data at rest and adequately securing the encryption keys so that the data cannot be decrypted by unauthorized users; and

d. Immediately applying patches once they were made available.

3447. A "least privileges" policy can limit an attacker who exploits a vulnerability from accessing large volumes of data. Limiting access via policies such as least privileges means that, even if a threat actor is able to exploit a vulnerability or even use a legitimate login to access the system, access to sensitive data will be limited. The large volume of records accessed and exfiltrated in the Data Breach indicates that this was not done, because it is highly unlikely that any login would have legitimate access to that amount of sensitive data.

3448. "Zero Trust" is a security model and set of system design principles that emphasize security verification in network environments. The core principle of Zero Trust is "never trust, always verify." Thus, unlike traditional security models that assume everything inside a network is safe, Zero Trust assumes threats can exist both inside and outside the network.

3449. Zero Trust security frameworks require all users, whether inside or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted access to applications and data.[858] Numerous standards provide guidelines to organizations implementing "zero-trust" security frameworks, including NIST SP 800-207,[859] NIST SP 800-205,[860] and the CISA zero trust maturity model.[861]

3450. Two aspects of Zero Trust are particularly applicable to the MOVEit Data Breach. The first is the network is segmented into smaller, secure zones to maintain separate access for different parts of the network. This reduces the lateral movement of attackers within the network. The second is continuously monitoring the security posture of all hardware and software on the network. This helps to detect and respond to threats in real time.

3451. The United States Cybersecurity & Infrastructure Security Agency published recommendations for mitigating the MOVEit vulnerability by "[g]rant[ing] admin privileges and

---

[858] *See, e.g.*, *Zero Trust, A revolutionary approach to Cyber or just another buzz word?*, Deloitte (2021), https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/deloitte-cyber-zero-trust.pdf; *see also* Venu Shastri, *Zero Trust Architecture*, CrowdStrike (June 28, 2023), https://www.oracle.com/security/what-is-zero-trust; https://www.crowdstrike.com/cybersecurity-101/zero-trust-security.

[859] NIST, *NIST SP 800-207 – Zero Trust Architecture*, CSRC (Aug. 2020), https://csrc.nist.gov/pubs/sp/800/207/final.

[860] NIST, *NIST SP 800-205 – Attribute Considerations for Access Control Systems*, CSRC (June 2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-205.pdf.

[861] *Zero Trust Maturity Model*, CISA (Apr. 2023), https://www.cisa.gov/sites/default/files/2023-04/CISA_Zero_Trust_Maturity_Model_Version_2_508c.pdf.

access only when necessary, establishing a software allow list that only executes legitimate applications."[862]

3452. Finally, following Progress's announcement of the first MOVEit vulnerability on May 31, 2023,[863] vendors and VCEs including Welltok Bellwether Defendants should have, but did not, immediately begin taking security measures. Welltok Bellwether Defendants' failure to adequately safeguard Welltok Bellwether Plaintiffs' and Class Members' Private Information resulted in that information being accessed or obtained by third-party cybercriminals.

E. Welltok failed to follow Progress's recommendations regarding secure configuration of the MOVEit software.

3453. The MOVEit software offers secure configurations that any customer could implement to make the system more secure and to mitigate that impact of this Breach.

3454. Progress made several additional recommendations to users of the MOVEit software, like Welltok, including:

a. Using consistency check and tamper check utilities to validate consistently and the audit log.

b. Review audit logs for any anomalous behavior. Such anomalous behavior includes:

1) Sign-ons from specific IP addresses;

2) APIs used; and

3) Modification of settings.

[862] *#StopRansomware: Cl0p Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, CISA (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[863] *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)*, Progress: Community (June 16, 2023), https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023.

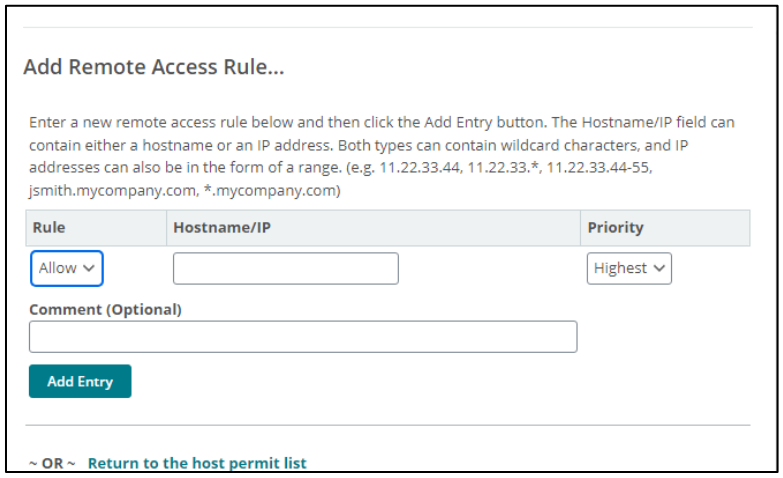
c. Limiting administrative privileges.[864]

d. IP and user lockout policies.[865]

e. Whitelisting so only specific IP addresses and users could login remotely.[866]

3455. Welltok could and should have turned on whitelisting:

Figure 46



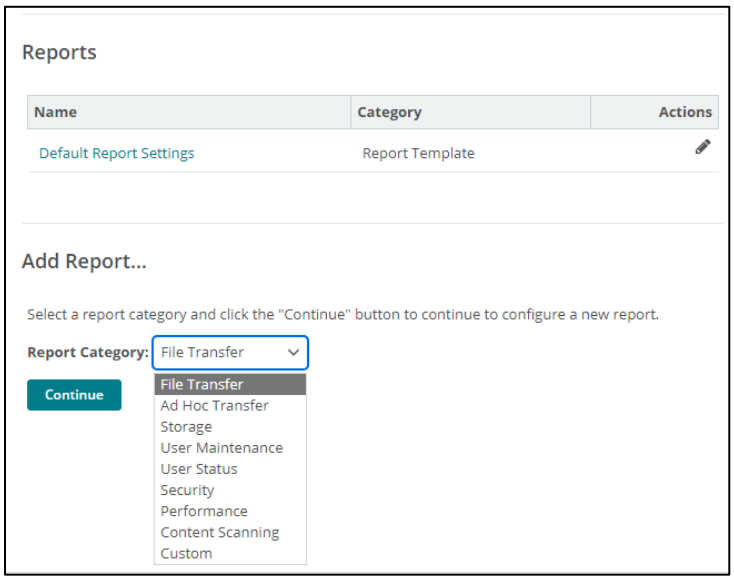
3456. Generating reports in MOVEit is also a simple process:

[864] *Progress Documentation: MOVEit Transfer 2022 Administrator Guide*, Progress, https://docs.progress.com/bundle/moveit-transfer-web-admin-help-2022/page/Permissions_3.html (last updated Apr. 6, 2022).

[865] *Progress Documentation: MOVEit Automation Web Admin Help – IP/User Lockout Policy*, Progress, https://docs.progress.com/bundle/moveit-automation-web-admin-help-2022/page/IPUser-Lockout-Policy.html (last updated Feb. 21, 2022).

[866] *MOVEit Transfer – Whitelist IP for Specific Users Accounts*, Progress: Community (Oct. 14, 2020), https://community.progress.com/s/article/moveit-transfer-whitelist-ip-for-specific-users-accounts.

Figure 47



3457. There are a number of security reports built into the MOVEit software:

Figure 48

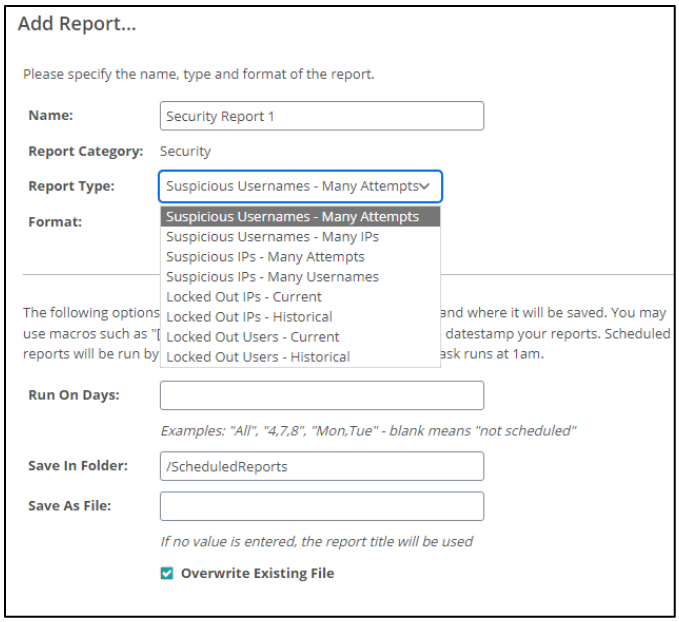
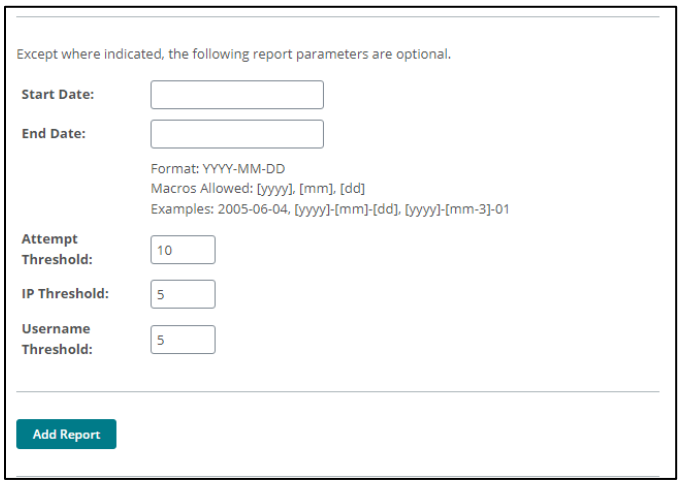
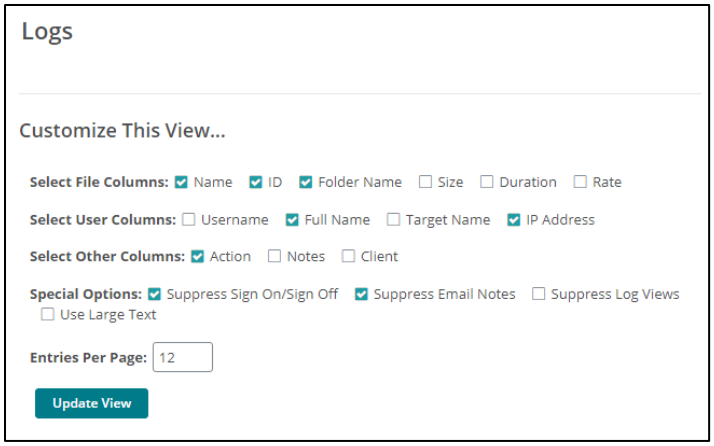


Figure 49



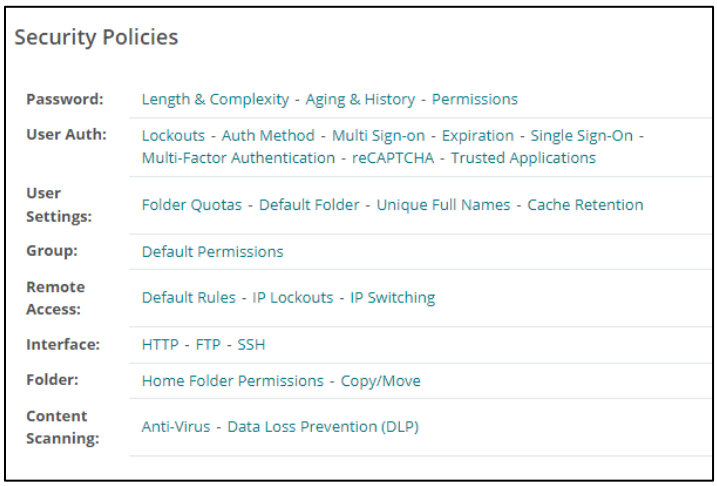
3458. MOVEit users can also customize the view of logs:

Figure 50



3459. A number of additional security policies can be set with a simple point and click:

Figure 51



3460. Data loss prevention rules could and should have been enabled to prevent exfiltration of data:

Figure 52

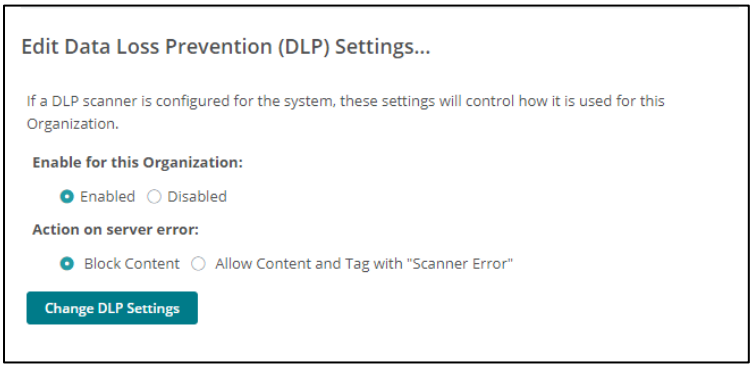


Figure 53

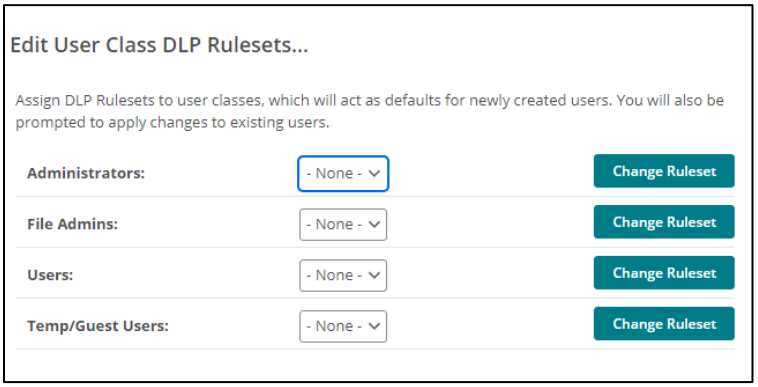
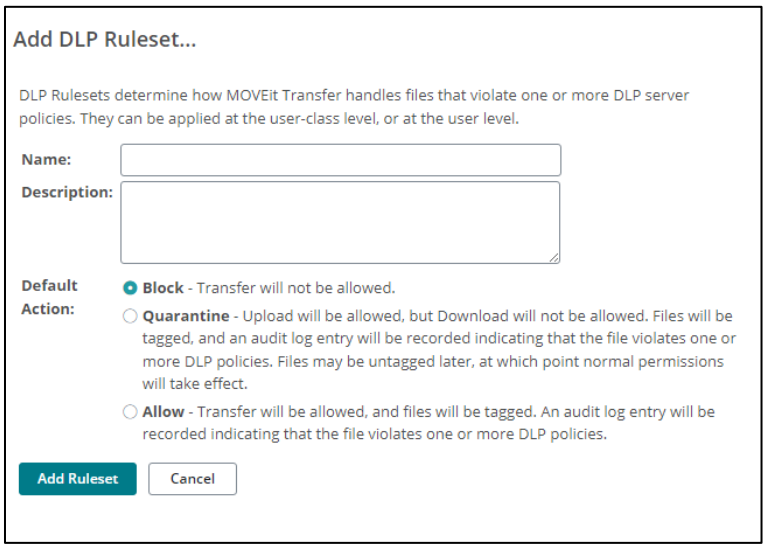


Figure 54



3461. It is unclear which, if any, of these security measures were implemented by Welltok.

F. Welltok chose to use the MOVEit software to transfer sensitive information despite its security flaws.

3462. Welltok enriched itself by saving the costs Welltok reasonably should have expended on adequate data security measures to secure Welltok Bellwether Plaintiffs' and Class Members' Private Information.

3463. Instead of providing a reasonable level of security that would have prevented the Data Breach, Welltok instead calculated to avoid their data security obligations at the expense of Welltok Bellwether Plaintiffs and Class Members by utilizing and relying on cheaper, ineffective security measures. Welltok Bellwether Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Welltok Bellwether Defendants' failures to provide the requisite security.

G. Welltok VCE Defendants chose to rely on Welltok to handle their sensitive information despite Welltok's security flaws and use of the MOVEit software.

3464. Similarly, Welltok VCE Defendants enriched themselves by saving the costs they reasonably should have expended on adequate data security measures to secure Welltok Bellwether Plaintiffs' and Class Members' Private Information and should have expended on oversight of Welltok's data security measures.

3465. Instead of providing a reasonable level of security that would have prevented the Data Breach, Welltok VCE Defendants instead calculated to avoid their data security obligations at the expense of Welltok Bellwether Plaintiffs and Class Members by relying on Welltok's ineffective security measures and failing to provide adequate oversight of Welltok's data security practices. Welltok Bellwether Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Welltok VCE Defendants' failures to provide the requisite security.

H. Welltok Bellwether Defendants' failures continued after the breach.

3466. Welltok Bellwether Defendants' failures were compounded by their inadequate response to the Data Breach.

3467. Despite CL0P successfully exploiting vulnerabilities in MOVEit Transfer and exfiltrating consumer data on May 30, 2023, from Welltok's MOVEit server, Welltok inexcusably did not discover that its MOVEit server was likely compromised until July 26, 2023, nearly two months after the Data Breach occurred.[867] That discovery occurred not because of Welltok's own diligence, but rather upon the alert of an unknown third-party.

[867] *Notice of Data Privacy Event*, Welltok (Oct. 24, 2023), https://welltoknotice.wpengine powered.com/?page_id=23.

3468. Welltok further did not confirm that CL0P had successfully accessed Welltok's MOVEit server until August 11, 2023, and did not confirm that Welltok Bellwether Plaintiffs' and Class Members' Private information had been exfiltrated by CL0P until August 26, 2023, three months after the Data Breach occurred.[868]

3469. Welltok further delayed notifying its Welltok Clients and Welltok Bellwether Plaintiffs and Class Members. On information and belief, Welltok did not notify its Welltok Clients of the Data Breach until on or about September 23, 2023 and did not provide a final report of its investigation into the Data Breach until on or about October 24, 2023.[869]

3470. Further compounding the negative consequences of the Data Breach, the Welltok Bellwether Defendants did not provide timely notice to affected individuals. Remarkably, the Welltok Bellwether Defendants did not begin to notify impacted individuals of the Data Breach until October 24, 2023, when Welltok published a press release on its website identifying impacted Welltok Clients, leaving victims to scour Welltok's list of clients to determine if they had been impacted.

3471. But Welltok obfuscated in publishing the press release. While the press release is linked to Welltok's website, upon information and belief, Welltok contemporaneously *removed nearly all content from its website*. Its website, welltok.com, now displays nothing more than a single line describing Welltok's business, along with a link to the press release about the Data Breach.[870] Further, one news organization's investigation found that Welltok's posted press release

---

[868] *Id.*

[869] *Sutter Health Vendor Reports Patient Information Incident*, Sutter Health (Nov. 3, 2023), https://vitals.sutterhealth.org/sutter-health-vendor-reports-patient-information-incident/.

[870] *See Welltok Homepage*, Welltok, www.welltok.com (last visited Dec. 2, 2024).

initially "include[d] 'noindex' code, which tells search engines to ignore the web page, effectively making it more difficult for affected customers to find the statement by searching for it."[871]

3472. Welltok failed to adequately and timely report the Data Breach, doing so through a series of filings and notifications, often separated by its various partner healthcare service providers.[872] Indeed, Welltok has issued at least seven separate batches of notifications to impacted consumers spanning a period between approximately October 24, 2023, and January 23, 2024, separated by its various partner healthcare service providers.[873]

3473. Welltok also failed to adequately report the severity and size of the Data Breach, initially reporting the Data Breach as affecting 8,493,379 individuals, but later, quietly updated its releases to report that the Data Breach actually affected 14,762,475 individuals.[874] As such, the size of the Data Breach effectively doubled between Welltok's initial announcement of the Data Breach on October 24, 2023 and a subsequent (and quiet update) to Health and Human Services at some point after April 2024.

3474. Welltok and Welltok VCE Defendants' notifications about the Data Breach were not timely, which allowed Welltok Bellwether Plaintiffs and Class Members' Private Information to be exposed for months before Welltok Bellwether Plaintiffs and Class Members had any idea

---

[871] Carly Page, *Hackers Accessed Sensitive Health Data of More Than 8 Million Welltok Patients*, TechCrunch (Nov. 20, 2023), https://techcrunch.com/2023/11/20/hackers-accessed-sensitive-health-data-of-welltok-patients/.

[872] *Id.*

[873] *See Data Breach* Notifications, Office of the Maine Attorney General (Jan. 23, 2024), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/cc3a6709-d064-4237-9b83-7fd510faf29e.shtml.

[874] Steve Adler, *Welltok Data Breach Victim Count Rises to 14.76 Million*, HIPAA Journal (Aug. 23, 2024), https://www.hipaajournal.com/welltok-data-breach/; Breach Portal, U.S. Department of Health & Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (sort by largest to smallest number of individuals affected to easily find Welltok, as it is the largest breach currently under HHS investigation).

their information was compromised. This prevented Welltok Bellwether Plaintiffs and Class Members from taking necessary precautions to prevent imminent and impending harms associated with the misuse of their Private Information.

3475. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires covered entities and business associates to provide notice of the Data Breach to each affected individual "***without unreasonable delay and in no case later than 60 days*** following discovery of the breach."[875]

3476. Several states set forth similar guidelines for timely notification of impacted individuals once an entity discovers a data breach, such as requiring entities to notify impacted consumers of a data breach "in the most expedient time possible, without unreasonable delay, and no more than thirty calendar days after the breach was discovered," unless law enforcement requests that the entity delay notification.[876]

3477. Although Welltok was aware of the Data Breach as early as July 2023 (and data theft occurred on May 30, 2023), Welltok and Welltok VCE Defendants failed to notify impacted individuals of the Data Breach until three months after the Data Breach was "discovered," and five months after the Data Breach occurred, in violation of HIPAA and these statutes, and further demonstrates the Welltok Bellwether Defendants' negligence.

3478. Welltok Bellwether Plaintiffs Copans and Meyer, for example, each received a Notice Letter by U.S. mail addressed to them directly from Welltok, writing on behalf of Sutter Health, dated October 31, 2023. According to the Notice Letter, Welltok Bellwether Plaintiff

[875] *Breach Notification Rule*, U.S. Dep't of Health & Human Servs., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last updated July 26, 2013).

[876] Wash. Rev. Code § 19.255.010.

Copans's and Plaintiff Meyer's Private Information was improperly accessed and obtained by unauthorized third parties, including their "name, date of birth, health insurance information, provider name, treatment cost information, and treatment information or diagnosis." Although the Notice Letter disclosed that on July 26, 2023, Welltok had been "alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool," it took Welltok and Sutter Health over *three months* to notify Welltok Bellwether Plaintiff Copans and Welltok Bellwether Plaintiff Meyer of the Data Breach.

3479. Welltok Bellwether Plaintiffs Williams and Weaver each received a Notice Letter by U.S. mail addressed to them directly from Welltok, writing on behalf of Corewell Health, dated November 17, 2023. According to the Notice Letter, Welltok Bellwether Plaintiff Williams's Private Information was improperly accessed and obtained by unauthorized third parties, including her "name, date of birth, email address, phone number, diagnosis, health insurance information, and Social Security Number." Welltok Bellwether Plaintiff Weaver received a similar Notice Letter. Although the Notice Letters disclosed that on July 26, 2023, Welltok had been "alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool," it took Welltok and Corewell Health *four months* to notify Welltok Bellwether Plaintiff Williams and Welltok Bellwether Plaintiff Weaver of the Data Breach.

3480. Welltok Bellwether Plaintiff Rehm received a Notice Letter by U.S. mail addressed to him directly from Welltok, writing on behalf of OSF, dated December 4, 2023. According to the Notice Letter, Welltok Bellwether Plaintiff Rehm's Private Information was improperly accessed and obtained by unauthorized third parties, including his "name and Date of Birth,

Treatment/Diagnosis." Although the Notice Letter disclosed that on July 26, 2023, Welltok had been "alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool," it took Welltok and OSF over *four months* to notify Welltok Bellwether Plaintiff Rehm of the Data Breach.

3481. Welltok Bellwether Plaintiff George received a Notice Letter by U.S. mail addressed to her directly from Welltok, writing on behalf of CHI, dated December 1, 2023. According to the Notice Letter, Welltok Bellwether Plaintiff George's Private Information was improperly accessed and obtained by unauthorized third parties, including her "name, address, date of birth, some clinical information, patient ID, and health insurance information." Although the Notice Letter disclosed that on July 26, 2023, Welltok had been "alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool," it took Welltok and CHI *over four months* to notify Welltok Bellwether Plaintiff George of the Data Breach.

3482. Welltok Bellwether Plaintiff McClendon received a Notice Letter by U.S. mail addressed to her directly from Welltok, writing on behalf of Virginia Mason, dated December 1, 2023. According to the Notice Letter, Welltok Bellwether Plaintiff McClendon's Private Information was improperly accessed and obtained by unauthorized third parties, including her "name, address, date of birth, some clinical information, patient ID, and health insurance information." Although the Notice Letter disclosed that on July 26, 2023, Welltok had been "alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool," it took Welltok and Virginia Mason over *four months* to notify Plaintiff McClendon of the Data Breach.

3483. Welltok Bellwether Plaintiff Rodda received a Notice Letter by U.S. mail addressed to her directly from Welltok, dated January 9, 2024. According to that Notice Letter, "Welltok operates an online contract-management platform that enables its healthcare clients, including Baylor Scott & White Health, to provide patients and members with important notices and communications, and received your information in connection with these services." Although the Notice Letter disclosed that on July 26, 2023, Welltok had been "alerted to an earlier alleged compromise of our MOVEit Transfer server in connection with software vulnerabilities made public by the developer of the MOVEit Transfer tool," it took Welltok *six months* to notify Welltok Bellwether Plaintiff Rodda of the Data Breach

3484. Welltok Bellwether Defendants' delay and obfuscation of important details in the wake of the Data Breach has compounded the harms suffered by victims—such as Welltok Bellwether Plaintiffs and the Class Members—as they seek clarity in a confusing, overwhelming, and often scary situation. Due to Welltok Bellwether Defendants' inadequate and incomplete release of information about the Breach, Welltok Bellwether Plaintiffs and the Class Members have been unable to mitigate the effects of the Breach.

3485. To date, critical details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again have not been explained or clarified to Welltok Bellwether Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

II. CLASS ALLEGATIONS AGAINST WELLTOK BELLWETHER DEFENDANTS

3486. Welltok Bellwether Plaintiffs Meyer, Copans, Rehm, Rodda, Williams, Weaver, McClendon, and George bring the causes of action listed below on behalf of themselves and, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) as representatives of the following proposed Welltok Class:

(1) Welltok Nationwide Class: All persons whose Private Information was compromised on Welltok's platform and/or systems in the MOVEit Data Breach.

3487. Welltok Bellwether Plaintiffs Meyer, Copans, Rehm, Rodda, Williams, Weaver, McClendon, and George also bring the causes of action listed below on behalf of themselves and on behalf of the following Welltok Subclasses:

(1) Welltok California Class: All residents of California whose Private Information was compromised on Welltok's platform and/or systems in the MOVEit Data Breach.

(2) Welltok Illinois Class: All residents of Illinois whose Private Information was compromised on Welltok's platform and/or systems in the MOVEit Data Breach.

(3) Welltok Texas Class: All residents of Texas whose Private Information was compromised on Welltok's platform and/or systems in the MOVEit Data Breach.

(4) Welltok Michigan Class: All residents of Michigan whose Private Information was compromised on Welltok's platform and/or systems in the MOVEit Data Breach.

(5) Welltok Nebraska Class: All residents of Nebraska whose Private Information was compromised on Welltok's platform and/or systems in the MOVEit Data Breach.

(6) Welltok Washington Class: All residents of Washington whose Private Information was compromised on Welltok's platform and/or systems in the MOVEit Data Breach.

The foregoing state-specific Welltok Classes are collectively referred to as the "Welltok State Classes."

3488. Welltok Bellwether Plaintiffs Meyer and Copans bring the causes of action listed below on behalf of themselves and, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) as representatives of the following proposed Sutter Health Classes:

(1) Sutter Health Nationwide Class: All persons whose Private Information was compromised in the MOVEit Data Breach which such information was obtained from or hosted by Sutter Health.

(a) Sutter Health California Class: All residents of California whose Private Information was compromised in the MOVEit Data Breach which such information was obtained from or hosted by Sutter Health.

3489. Welltok Bellwether Plaintiff Rehm brings the causes of action listed below on behalf of himself and, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) as representative of the following proposed OSF Classes:

(1) OSF Nationwide Class: All persons whose Private Information was compromised in the MOVEit Data Breach which such information was obtained from or hosted by OSF.

(a) OSF Illinois Class: All residents of Illinois whose Private Information was compromised in the MOVEit Data Breach which such information was obtained from or hosted by OSF.

3490. Welltok Bellwether Plaintiffs Williams and Weaver bring the causes of action listed below on behalf of themselves and, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) as representatives of the following proposed Corewell Classes:

(1) Corewell Nationwide Class: All persons whose Private Information was compromised in the MOVEit Data Breach which such information was obtained from or hosted by Corewell.

(b) Corewell Michigan Class: All residents of Michigan whose Private Information was compromised in the MOVEit Data Breach which such information was obtained from or hosted by Corewell.

3491. Welltok Bellwether Plaintiff George brings the causes of action listed below on behalf of herself and, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) as representative of the following proposed CHI Classes:

(1) CHI Nationwide Class: All persons whose Private Information was compromised in the MOVEit Data Breach which such information was obtained from or hosted by CHI.

(a) CHI Nebraska Class: All residents of Nebraska whose Private Information was compromised in the MOVEit Data Breach which such information was obtained from or hosted by CHI.

3492. Welltok Bellwether Plaintiff McClendon brings the causes of action listed below on behalf of herself and, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) as representative of the following proposed Virginia Mason Classes:

(1) Virginia Mason Nationwide Class: All persons whose Private Information was compromised in the MOVEit Data Breach which such information was obtained from or hosted by Virginia Mason.

(a) Virginia Mason Nebraska Class: All residents of Nebraska whose Private Information was compromised in the MOVEit Data Breach which such information was obtained from or hosted by Virginia Mason.

3493. Welltok Bellwether Plaintiff Rodda brings the causes of action listed below on behalf of herself and, pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), 23(b)(3), and 23(c)(4) as representative of the following proposed Baylor Scott Classes:

(2) Baylor Scott Nationwide Class: All persons whose Private Information was compromised in the MOVEit Data Breach which such information was obtained from or hosted by Baylor Scott.

(a) Baylor Scott Texas Class: All residents of Texas whose Private Information was compromised in the MOVEit Data Breach which such information was obtained from or hosted by Baylor Scott.

3494. All of the foregoing classes are referred to in this Chapter, collectively, as the "Welltok Bellwether Class." Excluded from the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Classes are: (1) the judges presiding over the action; (2) the Welltok Bellwether Defendants, their subsidiaries, parent companies, successors, predecessors, and any entity in which the Welltok Bellwether Defendants or their parents have a controlling interest, and their current or former officers and directors; (3) persons who properly opt out; and

(4) the successors or assigns of any such excluded persons.

3495. Welltok Bellwether Plaintiffs Meyer, Copans, Rehm, Rodda, Williams, Weaver, McClendon, and George reserve the right to, after conducting discovery, modify, expand, or amend the above Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Class definitions or to seek certification of classes or subclasses defined differently than above before any court determines whether certification is appropriate.

3496. The proposed Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Classes meet the criteria for certification under Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

3497. **Numerosity:** Welltok Bellwether Class Members are so numerous that their individual joinder is impracticable, as the proposed Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Classes are comprised of thousands if not millions of members who are geographically dispersed. The exact size of the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Classes and the identities of the individual members are identifiable through the Welltok Bellwether Defendants' records, including, but not limited to, the files implicated in the MOVEit Data Breach.

3498. **Typicality:** Welltok Bellwether Plaintiffs Meyer's Copans's, Rehm's, Rodda's, Williams's, Weaver's McClendon's, and George's claims are typical of the claims of the Welltok Bellwether Class Members. The claims of Welltok Bellwether Plaintiffs Meyer, Copans, Rehm, Rodda, Williams, Weaver, McClendon, and George are based on the same legal theories and arise from the same failure by Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason to safeguard their Private Information that was compromised in the MOVEit Data Breach.

3499. **Adequacy:** Welltok Bellwether Plaintiffs Meyer, Copans, Rehm, Rodda, Williams, Weaver, McClendon, and George are adequate representatives of the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Classes because Welltok Bellwether Plaintiffs Meyer, Copans, Rehm, Rodda, Williams, Weaver, McClendon, and George are each a member of the Classes they seek to represent and are committed to pursuing this matter against Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason on behalf of themselves and the Welltok Bellwether Class Members. Welltok Bellwether Plaintiffs Meyer, Copans, Rehm, Rodda, Williams, Weaver, McClendon, and George have no conflicts of interest with the Welltok Bellwether Class Members. Welltok Bellwether Plaintiffs Meyer, Copans, Rehm, Rodda, Williams, Weaver, McClendon, and George have also retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations.

3500. **Commonality and Predominance:** The following questions of law and fact are common to all Welltok Bellwether Class Members and predominate over any potential questions affecting individual Welltok Bellwether Class Members:

a. Whether the Welltok Bellwether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Welltok Bellwether Plaintiffs Meyer's Copans's, Rehm's, Rodda's, Williams's, Weaver's McClendon's, and George's and Welltok Bellwether Class Members' Private Information from unauthorized access and disclosure;

b. Whether the Welltok Bellwether Defendants failed to exercise reasonable care to secure and safeguard Welltok Bellwether Plaintiffs Meyer's Copans's, Rehm's, Rodda's, Williams's, Weaver's McClendon's, and George's and Welltok Bellwether Class Members' Private Information;

c. Whether the Welltok Bellwether Defendants breached their duties to protect Welltok Bellwether Plaintiffs Meyer's Copans's, Rehm's, Rodda's, Williams's, Weaver's McClendon's, and George's and Welltok Bellwether Class Members' Private Information;

d. Whether the Welltok Bellwether Defendants violated the statutes alleged herein;

e. Whether Welltok Bellwether Plaintiffs Meyer's Copans's, Rehm's, Rodda's, Williams's, Weaver's McClendon's, and George's and all other Welltok Bellwether Class Members are entitled to damages and the measure of such damages and relief.

3501. **Superiority:** A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Welltok Bellwether Plaintiffs Meyer's Copans's, Rehm's, Rodda's, Williams's, Weaver's McClendon's, and George's and other Welltok Bellwether Class Members' claims. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Welltok Bellwether Class Members individually to effectively redress the Welltok Bellwether Defendants' wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

3502. **Injunctive Relief Also Appropriate:** Consistent with Fed. R. Civ. P. 23(b)(2), the Welltok Defendants, through their uniform conduct, acted or refused to act on grounds generally applicable to the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Classes as a whole, making injunctive and declaratory relief appropriate to the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Classes as a whole.

III. CAUSES OF ACTION AGAINST WELLTOK BELLWETHER DEFENDANTS

WELLTOK BELLWETHER FIRST CLAIM FOR RELIEF
Negligence

(Brought on behalf of the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Nationwide Classes or, alternatively, the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason State Classes)

3503. Welltok Bellwether Plaintiffs re-allege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3504. Welltok Bellwether Plaintiffs bring this claim against Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason on behalf of the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Nationwide Classes or, in the alternative, the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason State Classes.

3505. Sutter Health, OSF, Baylor Scott, Corewell, CHI, Virginia Mason, and other Welltok Clients required Welltok Bellwether Plaintiffs and Class Members to entrust them with their Private Information in order to receive healthcare and/or health plan services. Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason, and other Welltok Clients collected, stored, and maintained the Private Information of Welltok Bellwether Plaintiffs and Class Members during the course of providing healthcare and/or health plan services.

3506. Sutter Health, OSF, Baylor Scott, Corewell, CHI, Virginia Mason, and other Welltok Clients collected, stored, maintained, and shared Welltok Bellwether Plaintiffs' and Class Members' Private Information with Welltok in connection with the services provided by Welltok to Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason, and other Welltok Clients.

3507. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason stored and transferred this vast treasure trove of Private Information via MOVEit Transfer to Welltok, and more specifically, Welltok's MOVEit server.

3508. In providing their Private Information, directly or indirectly, to Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, Virginia Mason, and other Welltok Clients, Welltok Bellwether Plaintiffs and Class Members had a reasonable expectation that this Information would be securely maintained, and not accessible to unauthorized third parties, or exfiltrated by cybercriminals.

3509. Further, Welltok Bellwether Plaintiffs and Class Members had a reasonable expectation that in the event of a data breach, Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason would provide timely and adequate notice to Welltok Bellwether Plaintiffs and Class Members, so that Welltok Bellwether Plaintiffs and Class Members could take prompt and appropriate steps to safeguard their identities.

3510. By actively collecting, storing, maintaining, transferring, and profiting from Welltok Bellwether Plaintiffs' and Class Members' Private Information, Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason each had a duty of care to Welltok Bellwether Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, transferring, safeguarding, and protecting this Private Information in the Welltok Bellwether Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized third parties.

3511. Pursuant to this duty, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason were required to: (i) affirmatively audit third-party software, including MOVEit Transfer, to identify vulnerabilities, monitor access to sensitive data, and discover and remediate

any unauthorized data access; (ii) affirmatively vet and audit the data security practices of third-party vendors, including the vetting of Welltok's and Progress's data security practices; (iii) affirmatively implement adequate supply chain security; (iv) and provide prompt and adequate notice to those affected by a data breach of Welltok Bellwether Plaintiffs' and Class Members' Private Information.

3512. Pursuant to this duty, Welltok was similarly required to: (i) affirmatively design, maintain, and test its security systems to ensure that these systems, including its MOVEit server, were reasonably secure and capable of protecting the Private Information of Welltok Bellwether Plaintiffs and Class Members; (ii) affirmatively implement systems and procedures that would detect a breach of its security systems, including its MOVEit server, in a timely manner and to timely act upon security alerts from such systems; (iii) affirmatively design, implement, and monitor data security systems, including their MOVEit server, policies, and processes to protect against reasonably foreseeable data breaches such as this Data Breach; (iv) affirmatively audit third-party software, including MOVEit Transfer, to identify vulnerabilities, monitor access to sensitive data, and discover and remediate any unauthorized data access; (v) affirmatively vet and audit the data security practices of third-party vendors, including the vetting of Progress's data security practices; and (vi) provide prompt and adequate notice to those affected by a data breach of their security systems.

3513. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason had common law duties to prevent foreseeable harm to Welltok Bellwether Plaintiffs and Class Members. These duties existed because Welltok Bellwether Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Welltok Bellwether Plaintiffs and Class Members would be harmed by the

Welltok Bellwether Defendants' affirmative implementation of inadequate security measures and failure to protect Private Information because hackers routinely target inadequately protected security systems the Private Information was stored therein in an attempt to steal such information and use it for nefarious purposes, the Welltok Bellwether Defendants knew it was more likely than not that Welltok Bellwether Plaintiffs and Class Members would be harmed by the Welltok Bellwether Defendants' inadequate data security measures and the theft of their Private Information.

3514. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason also owed common law duties because their conduct created a foreseeable risk of harm to Welltok Bellwether Plaintiffs and Class Members. The Welltok Bellwether Defendants' affirmative conduct included implementing inadequate data security measures to protect Welltok Bellwether Plaintiffs' and Class Members' Private Information.

3515. Welltok's duty also arose from its position as a "business associate" with the meaning of HIPAA of Sutter Health, OSF, Baylor Scott, Corewell, CHI, Virginia Mason, and other Welltok Clients. By collecting, maintaining, and transferring the Private Information of Welltok Bellwether Plaintiffs and Class Members in order to provide services to Sutter Health, OSF, Baylor Scott, Corewell, CHI, Virginia Mason, and other Welltok Clients, Welltok had a special relationship with Welltok Bellwether Plaintiffs and Class Members, and thereby assumed a duty to reasonably protect Welltok Bellwether Plaintiffs' and Class Members' Private Information as it was in a unique and superior position to protect against the harm suffered by Welltok Bellwether Plaintiffs and Class Members as a result of the Data Breach.

3516. Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's duty also arose from their positions as healthcare and health plan providers. By collecting and

maintaining Welltok Bellwether Plaintiffs' and Class Members' Private Information in order to provide healthcare and health plan services, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason have a special relationship with Welltok Bellwether Plaintiffs and Class Members, and thereby assumed a duty to reasonably protect Welltok Bellwether Plaintiffs' and Class Members' Private Information as they were in a unique and superior position to protect against the harm suffered by Welltok Bellwether Plaintiffs and Class Members as a result of the Data Breach.

3517. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason had duties to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

3518. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason had a duty to use reasonable security measures under HIPAA, which required Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

3519. Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's duty to act reasonably in collecting, storing, and maintaining the Private Information, and to use reasonable care in protecting such information arose not only as a result of the statutes and regulations described above, but also because Welltok, Sutter Health, OSF, Baylor Scott,

Corewell, CHI, and Virginia Mason are bound by industry standards to protect confidential Private Information that they either affirmatively acquire, maintain, stores, utilize, and/or transfer.

3520. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason were subject to an "independent duty," untethered to any contract between Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason and Welltok Bellwether Plaintiffs or Class Members.

3521. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason affirmatively breached their duties to Welltok Bellwether Plaintiffs in Class Members in numerous ways, as described herein, including by:

a. Acting unreasonably in collecting, storing, and maintaining the Private Information and failing to exercise reasonable care in their implementation of their security systems, protocols, and practices in order to sufficiently protect the Private Information of Welltok Bellwether Plaintiffs and Class Members;

b. Negligently designing and maintaining their data security systems in a manner that failed secure Welltok Bellwether Plaintiffs' and Class Members' Private Information from unauthorized access;

c. Inadequately monitoring the security of their networks and systems, including their MOVEit Transfer server;

d. Allowing unauthorized access to Welltok Bellwether Plaintiffs' and Class Members' Private Information;

e. Inadequately auditing third-party software, including MOVEit Transfer;

f. Inadequately vetting, auditing, monitoring, or ensuring the integrity of their vendor's data security practices;

g. Failing to detect in a timely manner that Welltok Bellwether Class Members' Private Information had been compromised; and

h. Failing to timely and adequately notify Welltok Bellwether Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

3522. A breach of security, unauthorized access, and resulting injury to Welltok

Bellwether Plaintiffs and the Class Members was reasonably foreseeable, particularly in light of Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's inadequate security practices.

3523. It was foreseeable that Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's failure to use reasonable measures to protect Welltok Bellwether Plaintiffs' and Class Members' Private Information would result in injury to Welltok Bellwether Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the administrative services and file transfer software industries.

3524. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason have full knowledge of the sensitivity of the Private Information and the types of harm that Welltok Bellwether Plaintiffs and the Class Members could and would suffer if their Private Information were wrongfully disclosed.

3525. Welltok Bellwether Plaintiffs and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason knew or should have known of the inherent risks in collecting and storing the Private Information of Welltok Bellwether Plaintiffs and the Class Members, the critical importance of providing adequate security of that Private Information, the necessity for encrypting Private Information stored on Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's systems, and adequately securing the encryption keys so that encrypted Private Information cannot be decrypted by unauthorized users.

3526. It was therefore foreseeable that the failure to adequately safeguard Welltok Bellwether Plaintiffs' Class Members' Private Information would result in one or more types of

injuries to Welltok Bellwether Plaintiffs' and Class Members.

3527. Welltok Bellwether Plaintiffs and the Class Members had no ability to protect their Private Information that was in, and possibly remains in, Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's possession.

3528. Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's duties extended to protecting Welltok Bellwether Plaintiffs and the Class Members from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

3529. But for Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's wrongful and negligent breach of duties owed to Welltok Bellwether Plaintiffs and the Class Members, the Private Information of Welltok Bellwether Plaintiffs and the Class Members would not have been compromised.

3530. There is a close causal connection between Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's inadequately implemented security measures to protect the Private Information of Welltok Bellwether Plaintiffs and the Class Members and the harm, or risk of imminent harm, suffered by Welltok Bellwether Plaintiffs and the Class Members. The Private Information of Welltok Bellwether Plaintiffs and the Class Members was lost and accessed as the proximate result of Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's failure to exercise reasonable care in safeguarding such Private Information by affirmatively adopting, implementing, and maintaining

inadequate security measures.

3531. The injury and harm that Welltok Bellwether Plaintiffs and the other Class Members suffered was the direct and proximate result of Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell, CHI's, and Virginia Mason's negligence. Welltok Bellwether Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—a risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) lost value of their Private Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks identity theft they face and will continue to face; (vi) out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; and (vii) anxiety and emotion distress as a result of the unauthorized disclosure of their Private Information and publication on the dark web.

3532. As a direct and proximate result of Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's negligence, Welltok Bellwether Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, nominal, and punitive damages in an amount to be proven at trial.

3533. Welltok Bellwether Plaintiffs and Class Members are also entitled to injunctive relief requiring Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to

future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to Welltok Bellwether Plaintiffs and Class Members.

WELLTOK BELLWETHER SECOND CLAIM FOR RELIEF
Negligence *per se*
(Brought on behalf of the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Nationwide Classes or, alternatively, the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason State Classes)

3534. Welltok Bellwether Plaintiffs re-allege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3535. Welltok Bellwether Plaintiffs bring this claim against Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason on behalf of the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Nationwide Classes or, in the alternative, the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason State Classes.

3536. Welltok's, Sutter Health's, OSF's, Baylor Scott's Corewell, CHI's, and Virginia Mason's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

3537. Welltok's, Sutter Health's, OSF's, Baylor Scott's Corewell, CHI's, and Virginia Mason's duties also arise from Section 5 of the FTCA, 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and

Virginia Mason, of failing to employ reasonable measures to protect and secure Private Information.

3538. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Welltok Bellwether Plaintiffs' and Class Members' Private Information and not complying with applicable industry standards. Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's conduct was particularly unreasonable given the nature and amount of Private Information they obtain and store, and the foreseeable consequences of a data breach involving Private Information including, specifically, the substantial damages that would result to Welltok Bellwether Plaintiffs and Class Members.

3539. Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's violations of the HIPAA Privacy and Security Rules and Section 5 of the FTCA constitute negligence *per se*.

3540. Welltok Bellwether Plaintiffs and Class Members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

3541. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against.

3542. It was reasonably foreseeable to Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason that their failure to exercise reasonable care in safeguarding and protecting Welltok Bellwether Plaintiffs' and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems,

would result in the access, compromise, and theft of Welltok Bellwether Plaintiffs' and Class Members' Private Information by unauthorized individuals.

3543. The injury and harm that Welltok Bellwether Plaintiffs and the other Class Members suffered was the direct and proximate result of Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's violations of HIPAA Privacy and Security Rules and Section 5 of the FTCA. Welltok Bellwether Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—a risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) lost value of their Private Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks identity theft they face and will continue to face; (vi) out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; and (vii) anxiety and emotion distress as a result of the unauthorized disclosure of their Private Information and publication on the dark web.

3544. As a direct and proximate result of Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's violation of the foregoing statutes and regulations, Welltok Bellwether Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, nominal, and punitive damages in an amount to be proven at trial.

3545. Welltok Bellwether Plaintiffs and Class Members are also entitled to injunctive relief requiring Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to

future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to Welltok Bellwether Plaintiffs and all Class Members.

WELLTOK BELLWETHER THIRD CLAIM FOR RELIEF
Breach of Third-Party Beneficiary Contract
(Brought on behalf of the Welltok Nationwide Class or, alternatively, the Welltok State Classes)

3546. Welltok Bellwether Plaintiffs re-allege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3547. Welltok Bellwether Plaintiffs bring this claim against Welltok on behalf of the Welltok Nationwide Class, or in the alternative, the Welltok State Classes.

3548. Welltok entered into written contracts with its Welltok Clients, including Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason, to provide patient engagement services and its patient activation platform to Welltok Bellwether Plaintiffs and Class Members.

3549. In exchange, Welltok agreed, in part, to implement adequate data security measures to safeguard the Private Information of Welltok Bellwether Plaintiffs and Class Members and to timely and adequately notify them of the Data Breach.

3550. These contracts were made expressly for the benefit of Welltok Bellwether Plaintiffs and the Class Members, as Welltok Bellwether Plaintiffs and Class Members were the intended third-party beneficiaries of the contracts entered into between Welltok and its Welltok Clients. Welltok knew that, if it were to breach these contracts with the Welltok Clients, the Clients' patients and employees—Welltok Bellwether Plaintiffs and Class Members—would be harmed.

3551. Welltok Bellwether Plaintiffs and Class Members are members of a class of people that the parties to the contracts intended to protect and benefit. Thus, Welltok Bellwether Plaintiffs and Class Members are third-party beneficiaries of such contracts.

3552. Welltok breached the contracts entered into with its Welltok Clients, by among other things, failing to: (i) use reasonable data security measures; (ii) implement adequate protocols and employee training sufficient to protect Welltok Bellwether Plaintiffs' and Class Members' Private Information from unauthorized disclosure to third parties; and (iii) promptly and adequately notify Welltok Bellwether Plaintiffs and Class Members of the Data Breach.

3553. As a direct and proximate result of Welltok's breach of contract, Welltok Bellwether Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—a risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) lost value of their Private Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks identity theft they face and will continue to face; (vi) out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; and (vii) anxiety and emotion distress as a result of the unauthorized disclosure of their Private Information and publication on the dark web.

3554. As a direct and proximate result of Welltok's breach of contract, Welltok Bellwether Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, nominal, and punitive damages in an amount to be proven at trial.

3555. Welltok Bellwether Plaintiffs and Class Members are also entitled to injunctive relief requiring Welltok to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to Welltok Bellwether Plaintiffs and Class Members.

WELLTOK BELLWETHER FOURTH CLAIM FOR RELIEF
Breach of Implied Contract
(Brought on behalf of the Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Nationwide Classes or, alternatively, the Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason State Classes)

3556. Welltok Bellwether Plaintiffs re-allege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3557. Welltok Bellwether Plaintiffs bring this claim against Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason on behalf of the Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Nationwide Classes, or in the alternative, the Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason State Classes.

3558. Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason acquired, stored, and maintained the Private Information of Welltok Bellwether Plaintiffs and the Class Members. Indeed, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason required Welltok Bellwether Plaintiffs and Class Members to provide, or authorize the transfer of, their Private Information in order to receive healthcare or health plan services from Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason.

3559. Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason offered, and invited Welltok Bellwether Plaintiffs and Class Members to provide their Private Information as

part of Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's regular business practices. Welltok Bellwether Plaintiffs and Class Members accepted these offers and provided their Private Information to Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason.

3560. Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing healthcare or health plan services to Welltok Bellwether Plaintiffs and Class Members.

3561. When Welltok Bellwether Plaintiffs and Class Members paid money to and provided their Private Information to Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason, either directly or indirectly, in exchange for goods or services, they entered into implied contracts with Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason.

3562. Implicit in the parties' agreement was that Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason would adequately safeguard the Private Information entrusted to them and would provide Welltok Bellwether Plaintiffs and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their Private Information.

3563. Welltok Bellwether Plaintiffs and the Class Members would not have entrusted their Private Information to Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason in the absence of such an agreement.

3564. Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason materially breached the contract(s) they had entered into with Welltok Bellwether Plaintiffs and Class Members by failing to safeguard such Private Information and failing to notify them promptly of the Data Breach that compromised such information. Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason further breached the implied contracts with Welltok Bellwether Plaintiffs

and Class Members by: (i) failing to properly safeguard and protect Welltok Bellwether Plaintiffs' and Class Members' Private Information; (ii) failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and (iii) failing to ensure the confidentiality and integrity of electronic Private Information that Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason created, received, maintained, and transmitted.

3565. The damages sustained by Welltok Bellwether Plaintiffs and Class Members as described above were the direct and proximate result of Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's material breaches of their implied agreement(s).

3566. Welltok Bellwether Plaintiffs and Class Members have performed as required under the relevant agreements, or such performance was waived by the conduct of Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason.

3567. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

3568. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

3569. Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason knew or should have known that Welltok Bellwether Plaintiffs and Class Members reasonably understood

that Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason would safeguard the Private Information Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason required Welltok Bellwether Plaintiffs and Class Members to disclose in order to provide healthcare and/or health plan services and communications to them through the Welltok platform used by Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason. Despite Welltok Bellwether Plaintiffs' and Class Members' reasonable expectations, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason failed to implement appropriate cybersecurity protocols to protect the Private Information from the Data Breach.

3570. In addition, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason failed to advise Welltok Bellwether Plaintiffs and Class Members of the Data Breach promptly and sufficiently, having waited months to send Welltok Bellwether Plaintiffs and other Class Members a notice letter, notifying them of the Data Breach.

3571. In these and other ways, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason violated their duties of good faith and fair dealing.

3572. As a direct and proximate result of Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's breach of contract and breach of the covenant of good faith and fair dealing, Welltok Bellwether Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—a risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) lost value of their Private Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the

effects of the Data Breach, including the increased risks identity theft they face and will continue to face; (vi) out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; and (vii) anxiety and emotion distress as a result of the unauthorized disclosure of their Private Information and publication on the dark web.

3573. As a direct and proximate result of Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's breach of contract and breach of the covenant of good faith and fair dealing, Welltok Bellwether Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, nominal, and punitive damages in an amount to be proven at trial.

3574. Welltok Bellwether Plaintiffs and Class Members are also entitled to injunctive relief requiring Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to Welltok Bellwether Plaintiffs and Class Members.

WELLTOK BELLWETHER FIFTH CLAIM FOR RELIEF
Unjust Enrichment
(Brought on behalf of the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Nationwide Classes, or alternatively, the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason State Classes)

3575. Welltok Bellwether Plaintiffs re-allege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3576. Welltok Bellwether Plaintiffs bring this claim in the alternative to the Welltok Bellwether Third Claim for Relief against Welltok on behalf of the Welltok Nationwide Class, or in the alternative, the Welltok State Class.

3577. Welltok Bellwether Plaintiffs bring this claim in the alternative to the Welltok Bellwether Fourth Claim for Relief against Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason on behalf of the Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Nationwide Classes, or in the alternative, the Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason State Classes.

3578. Welltok Bellwether Plaintiffs and Class Members have an interest, both equitable and legal, in their Private Information that was collected, stored, maintained by, and entrusted to Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason and that was ultimately compromised and/or stolen in the Data Breach.

3579. Upon information and belief, Welltok Bellwether Plaintiffs and Class Members conferred a monetary benefit upon Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason in the form of monies paid for healthcare and health plan services and from the receipt of Welltok Bellwether Plaintiffs' and Class Members' Private Information.

3580. Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason benefited by the conferral upon them of the monies paid for healthcare and health plan services and the Private Information pertaining to Welltok Bellwether Plaintiffs and Class Members, and by Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's ability to retain, use, and profit from that Information. Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason understood and valued these benefits.

3581. Upon information and belief Welltok Bellwether Plaintiffs and Class Members also conferred a monetary benefit upon Welltok by directly or indirectly entrusting their Private Information to Welltok. Welltok retained data and commercialized and used Welltok Bellwether Plaintiffs' and Class Members' Private Information for business purposes. Indeed, Welltok's

business model would not exist save for the need to ensure the security of Welltok Bellwether Plaintiffs' and Class Members' Private Information in order to provide their patient engagement services and their patient activation platform to their clients, Welltok Bellwether Plaintiffs, and Class Members.

3582. Welltok also benefitted by the conferral upon them of the Private Information pertaining to Welltok Bellwether Plaintiffs and Class Members and by their ability to retain, use, and profit from that Information. Welltok understood and valued this benefit.

3583. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason understood and appreciated that the Private Information pertaining to Welltok Bellwether Plaintiffs and Class Members was personal, private and confidential and its value depended upon Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason maintaining the privacy and confidentiality of that Private Information.

3584. The relationship between Welltok and Welltok Bellwether Plaintiffs and Class Members is not attenuated, as Welltok Bellwether Plaintiffs and Class Members had a reasonable expectation that the security of their Private Information would be maintained when they provided their Private Information to Sutter Health, OSF, Baylor Scott, Corewell, CHI, Virginia Mason, and other Welltok Clients.

3585. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason failed to secure Welltok Bellwether Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Welltok Bellwether Plaintiffs or Class Members for the value that their Private Information provided or for the monies paid for healthcare and/or health plan services.

3586. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason acquired the Private Information through inequitable means as they failed to disclose the inadequate data security practices previously alleged. If Welltok Bellwether Plaintiffs and Class Members had known that Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason would not fund adequate data security practices, procedures, and protocols to sufficiently monitor, supervise, and secure their Private Information, they would not have entrusted their Private Information to Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason.

3587. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Welltok Bellwether Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason instead calculated to increase their own profits at the expense of Welltok Bellwether Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to their own benefit. Welltok Bellwether Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's decision to prioritize their own profits over the requisite security and the safety of their Private Information.

3588. If Welltok Bellwether Plaintiffs and Class Members had known that Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their

Private Information, they would not have entrusted their Private Information at Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason.

3589. Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's unjust enrichment is traceable to and resulted directly and proximately from the conduct alleged herein, including the compiling and use of Welltok Bellwether Plaintiffs' and Class Members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

3590. It is inequitable, unfair, and unjust for Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason to retain these wrongfully obtained benefits. Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's retention of wrongfully obtained monies violates fundamental principles of justice, equity, and good conscience.

3591. The benefit conferred upon, received, and enjoyed by Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason was not conferred gratuitously, and it would be inequitable, unfair, and unjust for Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason to retain the benefit.

3592. Welltok Bellwether Plaintiffs and Class Members have no adequate remedy at law.

3593. As a direct and proximate result of Welltok Bellwether Defendants' wrongful conduct, Welltok Bellwether Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—a risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) lost value of their Private Information, for which there is a well-established

national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks identity theft they face and will continue to face; (vi) out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; and (vii) anxiety and emotion distress as a result of the unauthorized disclosure of their Private Information and publication on the dark web.

3594. Welltok Bellwether Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Welltok Bellwether Plaintiffs and Class Members may seek restitution or compensation.

WELLTOK BELLWETHER SIXTH CLAIM FOR RELIEF
Declaratory Judgment
(Brought on behalf of the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Nationwide Classes or, alternatively, the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason State Classes)

3595. Welltok Bellwether Plaintiffs re-allege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3596. Welltok Bellwether Plaintiffs bring this claim against Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason on behalf of the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Nationwide Classes or, in the alternative, the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason State Classes.

3597. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

3598. An actual controversy has arisen in the wake of the Data Breach regarding Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's present and prospective common law and other duties to reasonably safeguard Welltok Bellwether Plaintiffs' and Class Members' Private Information and whether Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason are currently maintaining data security measures adequate to protect Welltok Bellwether Plaintiffs and Class Members from further, future data breaches that compromise their Private Information.

3599. Welltok Bellwether Plaintiffs and Class Members allege that Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's data security measures remain inadequate and Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason have not provided any evidence that they have remedied the failure that occurred in the Data Breach at issue or have remedied any other vulnerability from their failure to properly assess threats by cybercriminals.

3600. Welltok Bellwether Plaintiffs and Class Members continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

3601. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason continue to owe a legal duty to secure consumers' Private

Information and to timely notify consumers of a data breach under the common law, the FTCA, and HIPAA;

b. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason owe a duty by virtue of their special relationship, understanding that they are safeguarding sensitive, Private Information, or that they have already acknowledged a responsibility to keep such information safe; and

c. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason continue to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

3602. The Court also should issue corresponding prospective injunctive relief requiring Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information.

3603. If an injunction is not issued, Welltok Bellwether Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason. The risk of another such breach is real, immediate, and substantial. If another breach at Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason occurs, Welltok Bellwether Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

3604. The hardship to Welltok Bellwether Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason if an injunction is issued. Among other things, if another massive data breach occurs at Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason, Plaintiffs and Class Members will likely be subjected to substantial identify theft and other damage (as they cannot elect to store their information with another company). On the other hand, the cost to Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason of complying with

an injunction by employing reasonable prospective data security measures is relatively minimal, and Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason have a pre-existing legal obligation to employ such measures.

3605. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by helping to prevent another data breach at Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason, thus eliminating the additional injuries that would result to Welltok Bellwether Plaintiffs and the millions of consumers whose Private Information would be further compromised.

WELLTOK BELLWETHER SEVENTH CLAIM FOR RELIEF
Violation of the California Consumer Privacy Act
Cal. Civ. Code §§ 1798.100 *et seq.*, § 1798.150(a)
(Brought on behalf of the Welltok California State Class)

3606. Welltok Bellwether Plaintiffs re-allege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3607. Welltok Bellwether Plaintiffs Meyer and Copans bring this claim against Welltok on behalf of the Welltok California State Class.

3608. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

> (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
>
> (B) Injunctive or declaratory relief.
>
> (C) Any other relief the court deems proper.

3609. Welltok is a "business" in that it is a corporation that is organized or operated for the profit or financial benefit of its shareholders or other owners, with annual gross revenues over $25 million.

3610. Welltok Bellwether Plaintiffs Meyer and Copans and Welltok California Class Members are "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

3611. Welltok is a business that collects consumers' personal information as defined by Cal. Civ. Code § 1798.140(e). Specifically, Welltok obtains, receives, or accesses consumers' personal information when providing patient engagement services.

3612. Welltok violated Section 1798.150 of the CCPA by failing to prevent Welltok Bellwether Plaintiffs Meyer and Copans and Welltok California Class Members' nonredacted Private Information from unauthorized access, decryption, exfiltration, theft, and/or disclosure as a result of Welltok's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the Information.

3613. Welltok knew or should have known that its computer systems, MOVEit server, and data security practices were inadequate to safeguard Welltok Bellwether Plaintiffs Meyer and Copans and Welltok California Class Members' Private Information and that the risk of a data breach or theft was highly likely. Welltok failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the Private

Information of Welltok Bellwether Plaintiffs Meyer and Copans and Welltok California Class Members. Specifically, Welltok subjected Welltok Bellwether Plaintiffs Meyer and Copans and Welltok California Class Members' nonredacted Private Information to unauthorized access decryption, exfiltration, theft, and/or disclosure as a result of the Welltok's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the Information, as described herein.

3614. The Private Information of Welltok Bellwether Plaintiffs Meyer and Copans and Welltok California Class Members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the Private Information Welltok collected and stored and which was impacted by the Data Breach include an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; or (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

3615. CL0P accessed and exfiltrated "nonencrypted and unredacted personal information" as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d), in the Data Breach.

3616. Upon information and belief, Welltok Bellwether Plaintiffs Meyer and Copans and Welltok California Class Members' Private Information that was accessed by, decrypted and

exfiltrated by CL0P in the Data Breach includes "nonencrypted and unredacted personal information" as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d).

3617. Welltok Bellwether Plaintiffs Meyer and Copans and Welltok California Class Members seek injunctive relief in the form of an order requiring Welltok to employ adequate security practices consistent with law and industry standards to protect Welltok Bellwether Plaintiffs Meyer and Copans and Welltok California Class Members' Private Information.

3618. Welltok Bellwether Plaintiffs Meyer and Copans and Welltok California Class Members seek statutory damages or actual damages, whichever is greater, pursuant to Cal. Civil Code § 1798.150(a)(1)(A).

3619. As a direct and proximate result of Welltok's violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Welltok Bellwether Plaintiffs Meyer and Copans and Welltok California Class Members' Private Information included exfiltration, theft, or disclosure through Welltok's servers, systems, and MOVEit sever, and/or the dark web, where hackers further disclosed the Private Information alleged herein.

3620. As a direct and proximate result of Welltok's acts, Welltok Bellwether Plaintiffs Meyer and Copans and Welltok California Class Members were injured and lost money or property, including, but not limited to, the loss of Welltok Bellwether Plaintiffs Meyer and Copans and Welltok California Class Members' legally protected interest in the confidentiality and privacy of their Private Information, stress, fear, and anxiety, nominal damages, and additional losses described above.

3621. Welltok Bellwether Plaintiffs Meyer and Copans have complied with the requirements of California Civil Code Section 1798.150(b), which provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual

pecuniary damages." On November 9, 2023, Welltok Bellwether Plaintiff Copans provided Welltok with written notice identifying Welltok's violations of Cal. Civil Code § 1798.150(a) and demanding the Data Breach be cured, pursuant to Cal. Civil Code § 1798.150(b). Similarly, on June 12, 2024, Welltok Bellwether Plaintiff Meyer provided Welltok with written notice identifying Welltok's violations of Cal. Civil Code § 1798.150(a) and demanding the Data Breach be cured, pursuant to Cal. Civil Code § 1798.150(b). Because Welltok has neither cured the noticed violation nor and provided the Welltok Bellwether Plaintiffs Meyer and Copans with an express written statement that the violations have been cured and that no further violations shall occur, Welltok Bellwether Plaintiffs Meyer and Copans and Welltok California Class Members seek statutory damages pursuant to Cal. Civil Code § 1798.150(a)(1)(A).

WELLTOK BELLWETHER EIGHTH CLAIM FOR RELIEF
Violation of the California Confidentiality of Medical Information Act
Cal. Civ. Code §§ 56, *et seq.*
(Brought on behalf of the Sutter Health Nationwide Class or, alternatively, the Welltok and Sutter Health California State Classes)

3622. Welltok Bellwether Plaintiffs re-allege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3623. Welltok Bellwether Plaintiffs Meyers and Copans bring this claim against Welltok and Sutter Health on behalf of the Sutter Health Nationwide Class and the Welltok and Sutter Health California State Classes ("California Class Members").

3624. The Confidentiality of Medical Information Act ("CMIA") prohibits, among other things, unauthorized disclosure of private medical information. Cal. Civ. Code §§ 56, *et seq*.

3625. Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members provided their Private Information to Sutter Health or another similar healthcare provider, each which are a "provider of health care" as defined by Cal. Civ. Code § 56.05(j).

3626. Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members are "patients" as defined by Cal. Civ. Code § 56.05(k).

3627. Welltok is subject to the CMIA because it is a "business that offers software or hardware to consumers, . . . that is designed to maintain medical information" in order to provide services to Sutter Health or other similar healthcare provider entities to which Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members provided their Private Information. Cal. Civ. Code § 56.06(b).

3628. At all relevant times, Welltok and Sutter Health collected, stored, managed, and transmitted Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members' Private Information.

3629. Welltok and Sutter Health stored in electronic form on their computer systems, Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members' "medical information" as defined by Cal. Civ. Code § 56.05(j).

3630. Welltok's platform was designed, in part, to make medical information available to Sutter Health and other similar entities by providing SaaS solutions and a patient engagement platform through which those organizations could store, access, and manage consumers' medical information, including, but not limited to, diagnosing, treating, or managing consumers' medical conditions.

3631. Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members did not provide Welltok or Sutter Health authorization nor were Welltok or Sutter Health otherwise

authorized to disclose Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members' medical information to an unauthorized third-party.

3632. As described throughout this Complaint, Welltok and Sutter Health negligently maintained, disclosed and released Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members' medical information inasmuch as they did not implement adequate security protocols to prevent unauthorized access to medical information, maintain an adequate electronic security system to prevent data breaches, or employ industry standard and commercially viable measures to mitigate the risks of any data breach or otherwise comply with HIPAA data security requirements.

3633. Welltok's and Sutter Health's conduct constitutes a violation of Sections 56.06 and 56.101 of the California CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential personal medical information.

3634. As a direct and proximate result of Welltok's and Sutter Health's negligence, they disclosed and released Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members' medical information to an unauthorized third-party.

3635. Welltok's and Sutter Health's unauthorized disclosure of medical records has caused injury to the Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members.

3636. Upon information and belief, Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members' confidential medical information was viewed by an unauthorized third party and published on the dark web.

3637. As a direct and proximate result of Welltok's and Sutter Health's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and

proximately caused the Data Breach and its violations of the CMIA, Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members are entitled to (i) actual damages, (ii) nominal damages of $1,000 per Welltok Bellwether Plaintiff Meyer and Copans and California Class Member, and (iii) attorneys' fees, litigation expenses and court costs under California Civil Code § 56.35.

WELLTOK BELLWETHER NINTH CLAIM FOR RELIEF
Violation of the California Customer Records, Act
Cal. Civ. Code § 1798.80 *et seq.*
(Brought on behalf of the Welltok and Sutter Health California Classes)

3638. Welltok Bellwether Plaintiffs re-allege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3639. Welltok Bellwether Plaintiffs Meyer and Copans bring this claim against Welltok and Sutter Health on behalf of the Welltok and Sutter Health California Classes ("California Class Members").

3640. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that Private Information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

3641. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

3642. Cal. Civ. Code § 1798.84(b) provides that "[a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

3643. Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to Welltok and Sutter Health for the purpose of obtaining healthcare services from Sutter Health and other clients of Welltok.

3644. Welltok and Sutter Health are each a business that owns, maintains, and licenses "personal information", within the meaning of Cal. Civ. Code § 1798.81.5(d)(1), about Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members.

3645. The Private Information of Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the Private Information Welltok and Sutter Health collect and which was impacted by the Data Breach includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not securely encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; or (vi) unique biometric data generated from measurements or

technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

3646. Moreover, Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay . . . ."

3647. Any person or business that is required to issue a security breach notification under the Customer Records Act must meet the following requirements under §1798.82(d):

a. The name and contact information of the reporting person or business subject to this section;

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

   i. the date of the breach,

   ii. the estimated date of the breach, or

   iii. the date range within which the breach occurred. The notification shall also include the date of the notice.

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information.

3648. Welltok and Sutter Health are each a business that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82(h).

3649. Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members' Private Information includes "personal information" as covered by Cal. Civ. Code §§ 1798.81.5(d)(1), 1798.82(h).

3650. The Data Breach described herein constituted a "breach of the security system" of Welltok and Sutter Health.

3651. Because Welltok and Sutter Health reasonably believed that Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members' Private Information was acquired by unauthorized persons during the Data Breach, Welltok and Sutter Health had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

3652. As alleged above, Welltok and Sutter Health unreasonably delayed informing Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members about the Data Breach, affecting their Private Information, after Welltok and Sutter Health knew that the Data Breach had occurred.

3653. By failing to disclose the Data Breach in a timely and accurate manner, Welltok and Sutter Health violated Cal. Civ. Code § 1798.82.

3654. As a result of Welltok's and Sutter Health's violation of Cal. Civ. Code § 1798.82, Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members because their stolen information would have had less value to identity thieves.

3655. As a result of Welltok's and Sutter Health's violation of Cal. Civ. Code § 1798.82, Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

3656. As a direct consequence of the actions as identified above, Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members incurred additional losses and suffered further harm to their privacy, including, but not limited to, economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

WELLTOK BELLWETHER TENTH CLAIM FOR RELIEF
Violation of California Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(Brought on behalf of the Sutter Health Nationwide Class, or alternatively, the Welltok and Sutter Health California State Classes)

3657. Welltok Bellwether Plaintiffs re-allege and incorporate by all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3658. Welltok Bellwether Plaintiffs Meyer and Copans bring this claim against Welltok and Sutter Health on behalf of the Sutter Health Nationwide Class or, in the alternative, the Welltok and Sutter Health California Classes ("California Class Members").

3659. Welltok and Sutter Health are each a "person" as defined by Cal. Bus. & Prof. Code § 17201.

3660. Welltok and Sutter Health violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

3661. Welltok's and Sutter Health's "unfair" acts and "deceptive" practices include:

a. Welltok and Sutter Health failed to implement and maintain reasonable security measures to protect Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Welltok and Sutter Health failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents.

b. Welltok's and Sutter Health's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTCA (15 U.S.C. § 45), HIPAA, 42 U.S.C. § 1320d, California's Consumer Records Act (Cal. Civ. Code § 1798.81.5), California's Consumer Legal Remedies Act (Cal Civ. Code § 1780, *et seq.*), and the Confidentiality of Medical Information Act (Cal Civ. Code § 56.26(b)).

c. Welltok's and Sutter Health's failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Welltok's, and Sutter Health's inadequate security, consumers could not have reasonably avoided the harms that Welltok and Sutter Health caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

3662. Welltok and Sutter Health have engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, *et. seq.* (requiring reasonable data security measures), California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTCA, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d.

3663. Welltok's and Sutter Health's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, HIPAA, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members' Private Information, including duties imposed by the FTCA Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*;

f. Failing to timely and adequately notify Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d., and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*

3664. Welltok's and Sutter Health's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Welltok's and Sutter Health's data security and ability to protect the confidentiality of consumers' Private Information.

3665. As a direct and proximate result of Welltok's and Sutter Health's unfair, unlawful, and fraudulent acts and practices, Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members were injured and lost money or property, including the costs passed through to Welltok and Sutter Health, the premiums and/or price received by Welltok and Sutter Health for their goods and services, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Private Information.

3666. Welltok and Sutter Health acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members' rights. Past file transfer data breaches

as well as other data breaches in the healthcare industry put them on notice that their security and privacy protections were inadequate.

3667. Unless restrained and enjoined, Welltok and Sutter Health will continue to engage in the above- described wrongful conduct and more data breaches will occur.

3668. Welltok's and Sutter Health's unfair and deceptive acts and practices complained of herein affected the public interest, including the large number of Californians affected by the Data Breach.

3669. As such, Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members seek restitution and an injunction, including public injunctive relief prohibiting Welltok and Sutter Health from continuing such wrongful conduct, and requiring Welltok and Sutter Health to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the Private Information entrusted to them, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

3670. To the extent any of these remedies are equitable, Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members seek such equitable remedies, in the alternative to any adequate remedy at law they may have, including under California's Consumer Privacy Act, California's Consumers Legal Remedies Act, California's Confidentiality of Medical Information Act, California's Customer Records Acts, and HIPAA.

WELLTOK BELLWETHER ELEVENTH CLAIM FOR RELIEF
Violation of the California Consumer Legal Remedies Act
Cal. Civ. Code §§ 1750, *et seq.*
(Brought on behalf of the Sutter Health Nationwide Class or, alternatively, the Welltok and Sutter Health California State Classes)

3671. Welltok Bellwether Plaintiffs re-allege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3672. Welltok Bellwether Plaintiffs Meyers and Copan bring this claim against Welltok and Sutter Health on behalf of the Sutter Health Nationwide Class or, in the alternative, the Welltok and Sutter Health California Classes ("California Class Members").

3673. At all relevant times, Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members were "consumers" as under the terms of the Consumer Legal Remedies Act ("CLRA") as individuals seeking or acquiring, by purchase or lease, goods or services for personal, family, or household purposes.

3674. At all relevant times Welltok's and Sutter Health's actions and conduct constituted transactions for the sale or lease of goods or services to consumers under the terms of the CLRA. The medical treatment and affiliated services offered and sold by Welltok and Sutter Health constitute "services" under the CLRA.

3675. By the acts described above, Welltok and Sutter Health violated California Civil Code section 1770(a)(5), by the use of untrue or misleading statements and omissions and representing that goods and services had characteristics or benefits they do not have.

3676. By the acts described above, Welltok and Sutter Health violated California Civil Code section 1770(a)(14), by representing that Sutter Health and Welltok maintained the highest

level of data security and a promise to safeguard Private Information from unauthorized use when Welltok and Sutter Health knew such rights were not conferred.

3677. Welltok and Sutter Health knew, or should have known, that their representations and advertisements about the nature of their data security were false or misleading and were likely to deceive a reasonable consumer. No reasonable consumer would use Welltok's and Sutter Health's products or engage Welltok's and Sutter Health's services if they knew Welltok and Sutter Health were not taking reasonable measures to safeguard their Private Information.

3678. Welltok's and Sutter Health's unfair and deceptive acts and practices complained of herein affected the public interest, including the large number of Californians affected by the Data Breach.

3679. As a direct and proximate result of Welltok's and Sutter Health's violations of California Civil Code § 1770, Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information, including, but not limited to, the diminishment of their present and future property interest in their Private Information and the deprivation of the exclusive use of their Private Information.

3680. Pursuant to California Civil Code § 1782(d), Welltok Bellwether Plaintiff Copans provided notice of her claims for damages to Welltok and Sutter Health on November 9, 2023. Similarly, Welltok Bellwether Plaintiff Meyer provided notice of his claims for damages to Welltok and Sutter Health on June 12, 2024. Welltok has neither cured the noticed violation nor

provided the Welltok Bellwether Plaintiffs Meyer or Copans with an express written statement that the violations have been cured and that no further violations shall occur.

3681. Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

WELLTOK BELLWETHER TWELFTH CLAIM FOR RELIEF
California Constitution's Right to Privacy
Cal. Const., Art. I, § I
(Brought by Welltok Bellwether Plaintiffs Meyer and Copans on behalf of the Welltok and Sutter Health California Classes against Welltok and Sutter Health)

3682. Welltok Bellwether Plaintiffs re-allege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3683. Welltok Bellwether Plaintiffs Meyer and Copans bring this claim against Welltok and Sutter Health on behalf of the Welltok and Sutter Health California Classes.

3684. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

3685. The right to privacy in California's Constitution creates a private right of action against private and government entities.

3686. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

3687. Welltok and Sutter Health violated Plaintiffs Welltok Bellwether Plaintiffs Meyer and Copans' and California Class Members' constitutional right to privacy by collecting, storing, and disclosing, or preventing from unauthorized disclosure, their personal identifying information and protected health information, which includes in which they had a legally protected privacy interest, and for which they had a reasonable expectation of privacy. Disclosure of their Private Information was highly offensive given the highly sensitive nature of the data. Disclosure of their private medical information in particular could cause humiliation to Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members. Accordingly, disclosure of Welltok Bellwether Plaintiffs Meyer and Copans' and California Class Members' Private Information is an egregious violation of social norms.

3688. Welltok and Sutter Health intruded upon Welltok Bellwether Plaintiffs Meyer and Copans' and California Class Members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential Private Information.

3689. Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members had a reasonable expectation of privacy in that: (i) their invasion of privacy occurred as a result of Welltok's and Sutter Health' lax and inadequate security practices with respect to securely collecting, storing, and using data, as well as preventing the unauthorized disclosure of their Private Information; (ii) Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members did not consent or otherwise authorize Welltok and Sutter Health to disclose their Private Information to parties responsible for the cyberattack; and (iii) Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members could not reasonably expect Welltok and Sutter Health would commit acts in violation of laws protecting their privacy.

3690. As a result of Welltok's and Sutter Health's actions, Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members have been damaged as a direct and proximate result of Welltok's and Sutter Health's invasion of their privacy and are entitled to just compensation.

3691. Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members suffered actual and concrete injury as a result of Welltok's and Sutter Health's violations of their privacy interests. Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members are entitled to appropriate relief, including damages to compensate them for the harms to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Welltok's and Sutter Health's invasions.

3692. Welltok Bellwether Plaintiffs Meyer and Copans and California Class Members seek appropriate relief for that injury, including, but not limited to, damages that will reasonably compensate them for the harm to their privacy interests as well as disgorgement of profits made by Welltok and Sutter Health as a result of their intrusions upon Welltok Bellwether Plaintiffs Meyer and Copans' and California Class Members' privacy.

WELLTOK BELLWETHER THIRTEENTH CLAIM FOR RELIEF
Illinois Private Information Protection Act
815 Ill. Comp. Stat. §§ 530/10(a), *et seq*.
(Brought on behalf of the Welltok and OSF Illinois State Classes)

3693. Welltok Bellwether Plaintiff re-alleges and incorporates by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3694. Welltok Bellwether Plaintiff Rehm brings this claim against Welltok and OSF on behalf of the Welltok and OSF Illinois State Classes ("Illinois Class Members".

3695. As entities that collect, disseminate, and otherwise deal with nonpublic Private Information, Welltok and OSF are each a Data Collector as defined in 815 Ill. Comp. Stat. § 530/5.

3696. Welltok Bellwether Plaintiff Rehm and Illinois Class Members' Private Information (*e.g.*, Social Security numbers) includes Private Information as covered under 815 Ill. Comp. Stat. § 530/5.

3697. As Data Collectors, Welltok and OSF are required to notify Welltok Bellwether Plaintiff Rehm and Illinois Class Members of a breach of their data security systems in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. § 530/10(a).

3698. The Data Breach described herein constituted a "breach of the security system" of Welltok and OSF.

3699. Because Welltok and OSF reasonably believed that Welltok Bellwether Plaintiff Rehm and Illinois Class Members' Private Information was acquired by unauthorized persons during the Data Breach, Welltok and OSF had an obligation to disclose the Data Breach in a timely and accurate fashion.

3700. As alleged above, Welltok and Sutter Health unreasonably delayed informing Welltok Bellwether Plaintiff Rehm and Illinois Class Members' about the Data Breach, affecting their Private Information, after Welltok and OSF knew that the Data Breach had occurred.

3701. By failing to disclose the Data Breach in the most expedient time possible and without unreasonable delay, Welltok and OSF violated 815 Ill. Comp. Stat. § 530/10(a).

3702. Pursuant to 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

3703. As a result of Welltok's and OSF's violation of 815 Ill. Comp. Stat. § 530/10(a), Welltok Bellwether Plaintiff Rehm and Illinois Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Welltok Bellwether Plaintiff Rehm and Illinois Class Members because their stolen information would have had less value to identity thieves.

3704. As a result of Welltok's and OSF's violation of 815 Ill. Comp. Stat. § 530/10(a), Welltok Bellwether Plaintiff Rehm and Illinois Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

3705. As a direct and proximate result of Welltok's and OSF's violations of 815 Ill. Comp. Stat. § 530/10(a), Welltok Bellwether Plaintiff Rehm and Illinois Class Members suffered damages, as described above.

3706. Welltok Bellwether Plaintiff Rehm and Illinois Class Members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because Welltok's and OSF's willful violations of 815 Ill. Comp. Stat. § 530/10(a), including actual damages, equitable relief, costs, and attorneys' fees.

WELLTOK BELLWETHER FOURTEENTH CLAIM FOR RELIEF
Illinois Consumer Fraud Act
815 Ill. Comp. Stat. §§ 505, *et seq*.
(Brought on behalf of the OSF Nationwide Class or, alternatively, the Welltok and OSF Illinois State Classes)

3707. Welltok Bellwether Plaintiff re-alleges and incorporates by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3708. Welltok Bellwether Plaintiff Rehm brings this claim against Welltok and OSF on behalf of the OSF Nationwide Class or, in the alternative, the Welltok and OSF Illinois State Classes ("Illinois Class Members").

3709. Welltok and OSF are each a "person" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

3710. Welltok Bellwether Plaintiff Rehm and Illinois Class Members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

3711. Welltok's and OSF's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

3712. Welltok's and OSF's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Welltok Bellwether Plaintiff Rehm and Illinois Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiff Rehm and Illinois Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Private Information Protection Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq*., and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Welltok Bellwether Plaintiff Rehm and Illinois Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiff Rehm and Illinois Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Private Information Protection Act, 815 Ill. Comp. Stat. §§

530/10(a), *et seq*., and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Failing to timely and adequately notify Welltok Bellwether Plaintiff Rehm and Illinois Class Members of the Breach;

g. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Welltok Bellwether Plaintiff Rehm and Illinois Class Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiff Rehm and Illinois Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, the Illinois Private Information Protection Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq*., and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

3713. Welltok's and OSF's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Welltok's and OSF's data security and ability to protect the confidentiality of consumers' Private Information.

3714. Welltok and OSF intended to mislead Welltok Bellwether Plaintiff Rehm and Illinois Class Members and induce them to rely on its misrepresentations and omissions.

3715. The above unfair and deceptive practices and acts by Welltok and OSF were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

3716. Welltok and OSF acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Welltok Bellwether Plaintiff Rehm and Illinois Class Members' rights. Past file transfer breaches as well as other healthcare industry breaches put them on notice that their security and privacy protections were inadequate.

3717. Welltok's and OSF's unfair and deceptive acts and practices complained of herein affected the public interest, including the large number of Illinoisans affected by the Data Breach.

3718. As a direct and proximate result of Welltok's and OSF's unfair, unlawful, and deceptive acts and practices, Welltok Bellwether Plaintiff Rehm and Illinois Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

3719. Welltok Bellwether Plaintiff Rehm and Illinois Class Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

WELLTOK BELLWETHER FIFTEENTH CLAIM FOR RELIEF
Illinois Uniform Deceptive Trade Practices Act
815 Ill. Comp. Stat. §§ 510/10/2, *et seq*.
(Brought on behalf of the OSF Nationwide Class or, alternatively, the Welltok and OSF Illinois State Classes)

3720. Welltok Bellwether Plaintiff re-alleges and incorporates by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3721. Welltok Bellwether Plaintiff Rehm brings this claim against Welltok and OSF on behalf of the OSF Nationwide Class or, in the alternative, the Welltok and OSF Illinois State Classes ("Illinois Class Members").

3722. Welltok and OSF are each a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

3723. Welltok and OSF engaged in deceptive trade practices in the conduct of their business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

3724. Welltok's and OSF's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Welltok Bellwether Plaintiff Rehm and Illinois Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiff Rehm and Illinois Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and the Illinois Private Information Protection Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq*., which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Welltok Bellwether Plaintiff Rehm and Illinois Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiff Rehm and Illinois Class Members' Private Information, including duties imposed by the FTCA Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and the Illinois Private Information Protection Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq*.;

f. Failing to timely and adequately notify Welltok Bellwether Plaintiff Rehm and Illinois Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Welltok Bellwether Plaintiff Rehm and Illinois Class Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiff Rehm and Illinois Class Members'

> Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and the Illinois Private Information Protection Act, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq*.

3725. Welltok's and OSF's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Welltok's and OSF's data security and ability to protect the confidentiality of consumers' Private Information.

3726. The above unfair and deceptive practices and acts by Welltok and OSF were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Welltok Bellwether Plaintiff Rehm and Illinois Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

3727. Welltok's and OSF's unfair and deceptive acts and practices complained of herein affected the public interest, including the large number of Illinoisans affected by the Data Breach.

3728. As a result of Welltok's and OSF's violations of the Illinois Uniform Deceptive Trade Practices Act, Welltok Bellwether Plaintiff Rehm and Illinois Class Members suffered damages, as described above, and are likely to suffer harm in the future from the deceptive conduct absent injunctive relief.

3729. As a direct and proximate result of Welltok's and OSF's unfair, unlawful, and deceptive acts and practices, Welltok Bellwether Plaintiff Rehm and Illinois Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

3730. Welltok Bellwether Plaintiff Rehm and Illinois Class Members have no adequate remedy at law for the injuries relating to Welltok's and OSF's continued possession of their Private Information with inadequate cybersecurity system and policies. A judgment for monetary damages

will not end Welltok's and OSF's inability to safeguard the Private Information of Welltok Bellwether Plaintiff Rehm and Illinois Class Members.

WELLTOK BELLWETHER SIXTEENTH CLAIM FOR RELIEF
Violation of Massachusetts General Laws, Ch. 93A
(Brought on behalf of the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Nationwide Classes)

3731. Welltok Bellwether Plaintiffs re-allege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3732. Welltok Bellwether Plaintiffs bring this claim against Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason on behalf of the Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason Nationwide Classes.

3733. M.G.L. ch. 93A § 2 provides that "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful." M.G.L. ch. 93A § 9 permits any consumer injured by a violation of M.G.L. ch. 93A § 2 to bring a civil action, including a class action, for damages and injunctive relief.

3734. Welltok Bellwether Plaintiffs allege that Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason committed unfair business acts and/or practices in violation of M.G.L. ch. 93A §§ 2 and 9.

3735. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason knew or should have known of the inherent risks in experiencing a data breach if they failed to maintain adequate systems and processes for keeping Welltok Bellwether Plaintiffs' and Class Members' Private Information safe and secure. Only Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason were in a position to ensure that they systems were sufficient to protect against harm to Welltok Bellwether Plaintiffs and Class Members resulting from a data

security incident such as the Data Breach; instead, Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason failed to implement such safeguards.

3736. Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's own conduct also created a foreseeable risk of harm to Welltok Bellwether Plaintiffs and Class Members and their Private Information. Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's misconduct included failing to adopt, implement, and maintain the systems, policies, and procedures necessary to prevent the Data Breach.

3737. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason acknowledged that their conduct created actual harm to Welltok Bellwether Plaintiffs and Class Members because Welltok Bellwether Plaintiffs and Class Members were instructed to monitor their accounts for fraudulent conduct and identity theft.

3738. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason knew, or should have known, of the risks inherent in disclosing, collecting, storing, accessing, and transmitting Private Information and the importance of adequate security because of, inter alia, the prevalence of data breaches.

3739. Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason failed to adopt, implement, and maintain fair, reasonable, or adequate security measures to safeguard Welltok Bellwether Plaintiffs' and Class Members' Private Information, failed to recognize in a timely manner the Data Breach, and failed to notify Welltok Bellwether Plaintiffs and Class Members in a timely manner that their Private Information was accessed in the Data Breach.

3740. These acts and practices are unfair in material respects, offend public policy, are

immoral, unethical, oppressive, and unscrupulous and violate 201 CMR 17.00 and M.G.L. ch. 93A § 2.

3741. The injury and harm that Welltok Bellwether Plaintiffs and the other Class Members suffered was the direct and proximate result of Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell, CHI's, and Virginia Mason's unfair acts and practices. Welltok Bellwether Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—a risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) lost value of their Private Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks identity theft they face and will continue to face; (vi) out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud; and (vii) anxiety and emotion distress as a result of the unauthorized disclosure of their Private Information and publication on the dark web.

3742. Neither Welltok Bellwether Plaintiffs nor the other Class Members contributed to the Data Breach.

3743. Welltok Bellwether Plaintiffs sent demands for relief, in writing to Welltok, Sutter Health, OSF, Baylor Scott, Corewell, CHI, and Virginia Mason on November 6, 2024 prior to filing this Complaint, as required by M.G.L. c. 93A § 9. Welltok Bellwether Plaintiffs have not received a written tender of settlement that is reasonable in relation to the injury actually suffered by Welltok Bellwether Plaintiffs and Class Members.

3744. Based on the foregoing, Welltok Bellwether Plaintiffs and the Class Members are entitled to all remedies available pursuant to M.G.L ch. 93A, including, but not limited to, refunds, actual damages, or statutory damages in the amount of twenty-five dollars per violation, whichever is greater, double or treble damages, attorneys' fees and other reasonable costs.

3745. Pursuant to M.G.L. ch. 231, § 6B, Welltok Bellwether Plaintiffs and Class Members are further entitled to pre-judgment interest as a direct and proximate result of Welltok's, Sutter Health's, OSF's, Baylor Scott's, Corewell's, CHI's, and Virginia Mason's wrongful conduct. The amount of damages suffered as a result is a sum certain and capable of calculation and Welltok Bellwether Plaintiffs and Class Members are entitled to interest in an amount according to proof.

WELLTOK BELLWETHER SEVENTEENTH CLAIM FOR RELIEF
Violation of the Michigan Identity Theft Protection Act
Mich. Comp. Laws Ann. § 445.72, *et seq.*
(Brought on behalf of the Welltok and Corewell Michigan State Classes)

3746. Welltok Bellwether Plaintiffs re-allege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3747. Welltok Bellwether Plaintiffs Williams and Weaver bring this claim against Welltok and Corewell on behalf of the Welltok and Corewell Michigan State Classes ("Michigan Class Members").

3748. As entities that collect, disseminate, and otherwise deal with nonpublic Private Information, Welltok and Corewell are each a "person or agency that owns or licenses data" of residents of the State of Michigan under Mich. Comp. Laws Ann. § 445.72(1)(a).

3749. Welltok Bellwether Plaintiffs Williams and Weaver's and Michigan Class Members' Private Information includes "personal information" as covered under Mich. Comp. Laws Ann. § 445.63(r).

3750. Welltok and Corewell are required to notify Welltok Bellwether Plaintiffs Williams and Weaver and Michigan Class Members of a breach of their data security system in the most expedient time possible and without unreasonable delay if a Michigan resident's unencrypted and unredacted personal information is accessed or acquired by an unauthorized person pursuant to Mich. Comp. Laws Ann. §§ 445.72(1)(a), (4).

3751. Upon information and belief, Welltok Bellwether Plaintiffs Williams and Weaver's and Michigan Class Members' unencrypted and unredacted personal information was accessed or compromised by CL0P during the Data Breach.

3752. The Data Breach described herein constituted a "breach of the security of a database" of Welltok and Corewell.

3753. Because Welltok and Corewell reasonably believed that Welltok Bellwether Plaintiffs Williams and Weaver's and Michigan Class Members' Private Information was acquired by unauthorized persons during the Data Breach, Welltok and Corewell had an obligation to disclose the Data Breach in a timely and accurate fashion.

3754. As alleged above, Welltok and Corewell unreasonably delayed informing Welltok Bellwether Plaintiffs Williams and Weaver and Michigan Class Members about the Data Breach, affecting their Private Information, after Welltok and Corewell knew that the Data Breach had occurred.

3755. By failing to disclose the Data Breach in the most expedient time possible and without unreasonable delay, Welltok and Corewell violated Mich. Comp. Laws Ann. §§ 445.72(1)(a), (4).

3756. As a result of Welltok's and Corewell's violation of Mich. Comp. Laws Ann. §§ 445.72(1)(a), (4), Welltok Bellwether Plaintiffs Williams and Weaver and Michigan Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Welltok Bellwether Plaintiffs Williams and Weaver and Michigan Class Members because their stolen information would have had less value to identity thieves.

3757. As a result of Welltok's and Corewell's violation of Mich. Comp. Laws Ann. §§ 445.72(1)(a), (4), Welltok Bellwether Plaintiffs Williams and Weaver and Michigan Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

3758. As a direct and proximate result of Welltok's and Corewell's violation of Mich. Comp. Laws Ann. §§ 445.72(1)(a), (4), Welltok Bellwether Plaintiffs Williams and Weaver and Michigan Class Members suffered damages, as described above.

3759. Welltok Bellwether Plaintiffs Williams and Weaver and Michigan Class Members seek relief under Michigan law pursuant to Mich. Comp. Laws Ann. § 445.72(15).

WELLTOK BELLWETHER EIGHTEENTH CLAIM FOR RELIEF
Michigan Consumer Protection Act
Mich Comp. Laws Ann. §§ 445.903, *et seq.*
(Brought on the behalf of the Corewell Nationwide Class or, alternatively, the Welltok and Corewell Michigan State Classes)

3760. Welltok Bellwether Plaintiffs re-allege and incorporate by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3761. Welltok Bellwether Plaintiffs Williams and Weaver bring this claim against Welltok and Corewell on behalf of the Corewell Nationwide Class or, in the alternative, the Welltok and Corewell Michigan State Classes ("Michigan Class Members").

3762. Welltok, Corewell, Welltok Bellwether Plaintiffs Williams and Weaver, and Michigan Class Members are "persons" as defined by Mich. Comp. Laws Ann. § 445.903(d).

3763. Welltok and Corewell advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

3764. Welltok and Corewell engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

a. Representing that their goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c);

b. Representing that their goods and services are of a particular standard or quality if they are of another in violation of Mich. Comp. Laws Ann. § 445.903(1)(e);

c. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb); and

d. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).

3765. Welltok's and Corewell's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Welltok Bellwether Plaintiffs Williams and Weaver and Michigan Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiffs Williams and Weaver and Michigan Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Welltok Bellwether Plaintiffs Williams and Weaver and Michigan Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiffs Williams and Weaver and Michigan Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d;

f. Failing to timely and adequately notify the Welltok Bellwether Plaintiffs Williams and Weaver and Michigan Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Welltok Bellwether Plaintiffs Williams and Weaver and Michigan Class Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiffs Williams and Weaver and Michigan Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d.

3766. Welltok and Corewell intended to mislead Welltok Bellwether Plaintiffs Williams and Weaver and Michigan Class Members and induce them to rely on their misrepresentations and omissions.

3767. Welltok and Corewell acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Welltok Bellwether Plaintiffs Williams and Weaver and Michigan Class Members' rights.

3768. Welltok's and Corewell's unfair and deceptive acts and practices complained of herein affected the public interest, including the large number of Michiganders affected by the Data Breach.

3769. As a direct and proximate result of Welltok's and Corewell's unfair, unconscionable, and deceptive practices, Welltok Bellwether Plaintiffs Williams and Weaver and Michigan Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

3770. Welltok Bellwether Plaintiffs Williams and Weaver and Michigan Class Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250, injunctive relief, and any other relief that is just and proper.

WELLTOK BELLWETHER NINETEENTH CLAIM FOR RELIEF
Nebraska Consumer Protection Act
Neb. Rev. Stat. §§ 59-1601, *et seq.*
(Brought on behalf of the CHI Nationwide Class or, alternatively, the Welltok and CHI Nebraska State Classes)

3771. Welltok Bellwether Plaintiff re-alleges and incorporates by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3772. Welltok Bellwether Plaintiff George brings this claim against Welltok and CHI on behalf of the CHI Nationwide Class, or in the alternative the Welltok and CHI Nebraska State Classes ("Nebraska Class Members").

3773. Welltok, CHI, Welltok Bellwether Plaintiff George, and Nebraska Class Members are each a "person" as defined by Neb. Rev. Stat. § 59-1601(1).

3774. Welltok and CHI advertised, offered, or sold goods or services in Nebraska and engaged in trade or commerce directly or indirectly affecting the people of Nebraska, as defined by Neb. Rev. Stat. § 59-1601.

3775. Welltok and CHI engaged in unfair and deceptive acts and practices in conducting trade and commerce, in violation of Neb. Rev. Stat. § 59-1602, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Welltok Bellwether Plaintiff George and Nebraska Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiff George and Nebraska Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and the Nebraska Data Protection Act, Neb. Rev. Stat. § 87-808, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Welltok Bellwether Plaintiff George and Nebraska Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiff George and Nebraska Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and the Nebraska Data Protection Act, Neb. Rev. Stat. § 87-808;

f. Failing to timely and adequately notify the Welltok Bellwether Plaintiff George and Nebraska Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Welltok Bellwether Plaintiff George and Nebraska Class Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiff George and Nebraska Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and the Nebraska Data Protection Act, Neb. Rev. Stat. § 87-808.

3776. Welltok's and CHI's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Welltok's and CHI's data security and ability to protect the confidentiality of consumers' Private Information.

3777. As a direct and proximate result of Welltok's and CHI's unfair and deceptive acts and practices, Welltok Bellwether Plaintiff George and Nebraska Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

3778. Welltok's and CHI's unfair and deceptive acts and practices complained of herein affected the public interest, including the large number of Nebraskans affected by the Data Breach.

3779. Welltok Bellwether Plaintiff George and Nebraska Class Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, the greater of either (1) actual damages or (2) $1,000, civil penalties, and reasonable attorneys' fees and costs.

WELLTOK BELLWETHER TWENTIETH CLAIM FOR RELIEF
Nebraska Uniform Deceptive Trade Practices Act
Neb. Rev. Stat. §§ 87-301, *et seq.*
(Brought on behalf of the CHI Nationwide Class or, alternatively, the Welltok and CHI Nebraska State Classes)

3780. Welltok Bellwether Plaintiff re-alleges and incorporates by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3781. Welltok Bellwether Plaintiff George brings this claim against Welltok and CHI on behalf of the CHI Nationwide Class, or in the alternative the Welltok and CHI Nebraska State Classes ("Nebraska Class Members").

3782. Welltok, CHI, Welltok Bellwether Plaintiff George, and Nebraska Class Members are each a "person" as defined by Neb. Rev. Stat. § 87-301(19).

3783. Welltok and CHI advertised, offered, or sold goods or services in Nebraska engaged in trade or commerce directly or indirectly affecting the people of Nebraska.

3784. Welltok and CHI engaged in unfair and deceptive acts and practices in conducting trade and commerce, in violation of Neb. Rev. Stat. §§ 87-302(a)(5), (8), and (10), including:

a. Represented that goods and services have characteristics, uses, benefits, or qualities that they do not have;

b. Represented that goods and services are of a particular standard, quality, or grade if they are of another; and

c. Advertised its goods and services with intent not to sell them as advertised and in a manner calculated or tending to mislead or deceive.

3785. Welltok's and CHI's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Welltok Bellwether Plaintiff George and Nebraska Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiff George and Nebraska Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and the Nebraska Data Protection Act, Neb. Rev. Stat. § 87-808, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Welltok Bellwether Plaintiff George and Nebraska Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiff George and Nebraska Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and the Nebraska Data Protection Act, Neb. Rev. Stat. § 87-808;

f. Failing to timely and adequately notify the Welltok Bellwether Plaintiff George and Nebraska Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Welltok Bellwether Plaintiff George and Nebraska Class Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiff George and Nebraska Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and the Nebraska Data Protection Act, Neb. Rev. Stat. § 87-808.

3786. Welltok's and CHI's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Welltok's and CHI's data security and ability to protect the confidentiality of consumers' Private Information.

3787. Welltok and CHI intended to mislead Welltok Bellwether Plaintiff George and Nebraska Class Members and induce them to rely on its misrepresentations and omissions.

3788. Had Welltok and CHI disclosed to Welltok Bellwether Plaintiff George and Nebraska Class Members that their data systems were not secure and, thus, vulnerable to attack, Welltok and CHI would have been unable to continue in business and they would have been forced to adopt reasonable data security measures and comply with the law. Instead, Welltok and CHI were trusted with sensitive and valuable Private Information of consumers' including Welltok Bellwether Plaintiff George and Nebraska Class Members. Welltok and CHI accepted the responsibility of being a steward of this data while keeping the inadequate state of their security controls secret from the public. Accordingly, because Welltok and CHI held themselves out as securely maintaining the Private Information, Welltok Bellwether Plaintiff George and Nebraska Class Members acted reasonably in relying on Welltok's and CHI's misrepresentations and omissions, the truth of which they could not have discovered.

3789. Welltok and CHI acted intentionally, knowingly, and maliciously to violate Nebraska's Uniform Deceptive Trade Practices Act, and recklessly disregarded Welltok Bellwether Plaintiff George and Nebraska Class Members' rights.

3790. As a direct and proximate result of Welltok's and CHI's unfair and deceptive acts and practices, Welltok Bellwether Plaintiff George and Nebraska Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

3791. Welltok's and CHI's unfair and deceptive acts and practices complained of herein affected the public interest, including the large number of Nebraskans affected by the Data Breach.

3792. Welltok Bellwether Plaintiff George and Nebraska Class Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, civil penalties, and attorneys' fees and costs.

WELLTOK BELLWETHER TWENTY-FIRST CLAIM FOR RELIEF
Washington Data Breach Notification Act
Wash. Rev. Code §§ 19.255.010, *et seq*.
(Brought on behalf of the Welltok and Virginia Mason Washington State Classes)

3793. Welltok Bellwether Plaintiff re-alleges and incorporates by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3794. Welltok Bellwether Plaintiff McClendon brings this claim against Welltok and Virginia Mason on behalf of the Welltok and Virginia Mason Washington State Classes ("Washington Class Members").

3795. As entities that collect, disseminate, and otherwise deal with nonpublic Private Information, Welltok and Virginia Mason are each a business that owns, licenses, or maintains computerized data that includes "Personal Information" as defined by Wash. Rev. Code § 19.255.005(2)(a) and Wash. Rev. Code § 19.255.010(1).

3796. Welltok Bellwether Plaintiff McClendon's and Washington Class Members' Private Information includes Private Information as "Personal Information" as defined by Wash. Rev. Code § 19.255.005(2)(a) and Wash. Rev. Code § 19.255.010(1).

3797. As businesses that own, license, or maintain computerized data that includes "Personal Information," Welltok and Virginia Mason are required to accurately notify Welltok Bellwether Plaintiff McClendon and Washington Class Members of a breach of their data security

system if "Personal Information" was, or is reasonably believed to have been, acquired by an unauthorized person and the "Personal Information" was not secured, in the most expedient time possible and without unreasonable delay pursuant to Wash. Rev. Code §§ 19.255.010(1), (2).

3798. The Data Breach described herein constituted a "breach of the security of the system" of Welltok and Virginia Mason as defined by Wash. Rev. Code § 19.255.005(1).

3799. Because Welltok and Virginia Mason reasonably believed that Welltok Bellwether Plaintiff McClendon's and Washington Class Members' Private Information was acquired by unauthorized persons during the Data Breach, Welltok and Virginia Mason had an obligation to disclose the Data Breach in a timely and accurate fashion.

3800. Upon information and belief, Welltok Bellwether Plaintiff McClendon's and Washington Class Members' Private information was not secured and was accessed or compromised by CL0P during the Data Breach.

3801. As alleged above, Welltok and Virginia Mason unreasonably delayed informing Welltok Bellwether Plaintiff McClendon and Washington Class Members about the Data Breach, affecting their Private Information, after Welltok and Virginia Mason knew that the Data Breach had occurred.

3802. By failing to disclose the Data Breach in the most expedient time possible and without unreasonable delay, Welltok and Virginia Mason violated Wash. Rev. Code §§ 19.255.010(1), (2).

3803. As a result of Welltok's and Virginia Mason's violation of Wash. Rev. Code §§ 19.255.010(1), (2), Welltok Bellwether Plaintiff McClendon and Washington Class Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These

measures could have prevented some of the damages suffered by Welltok Bellwether Plaintiff McClendon and Washington Class Members because their stolen information would have had less value to identity thieves.

3804. As a result of Welltok's and Virginia Mason's violation of Wash. Rev. Code §§ 19.255.010(1), (2), Welltok Bellwether Plaintiff McClendon and Washington Class Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

3805. As a direct and proximate result of Welltok's and Virginia Mason's violations of Wash. Rev. Code §§ 19.255.010(1), (2), Welltok Bellwether Plaintiff McClendon and Washington Class Members suffered damages, as described above.

3806. Welltok Bellwether Plaintiff McClendon and Washington Class Members seek relief under Wash. Rev. Code §§ 19.255.010(1), (2) for the harm they suffered because Welltok's and Virginia Mason's willful violations of Wash. Rev. Code §§ 19.255.040(3)(a), (b), including actual damages, equitable relief, costs, and attorneys' fees.

WELLTOK BELLWETHER TWENTY-SECOND CLAIM FOR RELIEF
Washington Consumer Protection Act
Wash Rev. Code §§ 19.86.020, *et seq*.
(Brought on behalf of the Virginia Mason Nationwide Class or, alternatively, the Welltok and Virginia Mason Washington State Classes)

3807. Welltok Bellwether Plaintiff re-alleges and incorporates by reference all paragraphs within the following sections: Preamble, Introduction, Parties, Jurisdiction and Venue, Chapter One, and Chapter Six.

3808. Welltok Bellwether Plaintiff McClendon brings this claim against Welltok and Virginia Mason on behalf of the Virginia Mason Nationwide Class or, in the alternative, the Welltok and Virginia Mason Washington State Classes ("Washington Class Members").

3809. Welltok and Virginia Mason are each a "person" as defined by Wash. Rev. Code Ann. § 19.86.010(1).

3810. Welltok and Virginia Mason advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010(2).

3811. Welltok and Virginia Mason engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Welltok Bellwether Plaintiff McClendon's and Washington Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiff McClendon's and Washington Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Welltok Bellwether Plaintiff McClendon's and Washington Class Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiff McClendon's and Washington Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d;

f. Failing to timely and adequately notify the Welltok Bellwether Plaintiff McClendon and Washington Class Members of the Data Breach;

g. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Welltok Bellwether Plaintiff McClendon's and Washington Class Members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Welltok Bellwether Plaintiff McClendon's and Washington Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, and HIPAA, 42 U.S.C. § 1320d.

3812. Welltok's and Virginia Mason's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Welltok's and Virginia Mason's data security and ability to protect the confidentiality of consumers' Private Information.

3813. Welltok and Virginia Mason acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Welltok Bellwether Plaintiff McClendon's and Washington Class Members' rights. Welltok and Virginia Mason are of such a sophisticated and large nature that other data breaches and public information regarding security vulnerabilities put them on notice that their security and privacy protections were inadequate.

3814. Welltok's and Virginia Mason's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, their conduct affected the public interest, including the many Washingtonians affected by the Data Breach.

3815. As a direct and proximate result of Welltok's and Virginia Mason's unfair and deceptive acts and practices, Welltok Bellwether Plaintiff McClendon and Washington Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

3816. Welltok Bellwether Plaintiff McClendon and Washington Class Members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

IV. PRAYER FOR RELIEF AS AGAINST WELLTOK BELLWETHER DEFENDANTS

3817. Plaintiffs, individually and on behalf of the Welltok Bellwether Class, respectfully request that the Court grant the following relief:

a. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiffs as Class Representative and undersigned counsel as Class Counsel;

b. Find in favor of Plaintiffs and the Classes on all counts asserted herein;

c. Award Plaintiffs and the Classes actual, statutory, and/or punitive monetary damages to the maximum extent as allowed by law;

d. Award Plaintiffs and the Classes compensatory, consequential, general, and/or nominal monetary damages in an amount to be proven at trial;

e. Award Plaintiffs and the Classes restitution and all other applicable forms of equitable monetary relief;

f. Award Plaintiffs and the Classes equitable relief by enjoining Welltok from engaging in the wrongful conduct complained of herein regarding the misuse or disclosure of the private information of Plaintiffs and Class Members, and by requiring Welltok to issue prompt, complete, and accurate disclosure to Plaintiffs and Class Members;

g. Award Plaintiffs and the Classes injunctive relief as permitted by law or equity to assure that they have an effective remedy, and to protect the interests of Plaintiffs and Class Members, including, but not limited to, an order:

    i. requiring Welltok to protect from unauthorized disclosure all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws, including by adequate encryption of all such data and by preventing unauthorized access to decryption keys;

    ii. requiring Welltok to delete, destroy, and purge any personal identifying information of Plaintiffs and Class Members in its possession unless Welltok can provide to the Court reasonable

justification for the retention and use of such information when weighted against the privacy interests of Plaintiffs and Class Members;

iii. requiring Welltok to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Welltok's systems on a periodic basis, and ordering Welltok to promptly correct any problems or issues detected by such third-party security auditors;

iv. requiring Welltok to engage independent third-party security auditors and internal personnel to run automated security monitoring including, but not limited to, regular database scanning and securing checks;

v. requiring Welltok to audit, test, and train its security personnel regarding any new or modified procedures;

vi. requiring Welltok to segment data by, among other things, creating firewalls and access controls so that if one area of Welltok network is compromised, hackers cannot gain access to other portions of Welltok's systems;

vii. requiring Welltok to establish for all Welltok employees an information security training program that includes annual training, with additional training to be provided as appropriate;

viii. requiring Welltok to establish for all Welltok security personnel a security training program that includes regularly scheduled internal training and education to inform Welltok's internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

ix. requiring Welltok to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Welltok's policies, programs, and systems for protecting personal identifying information;

x. requiring Welltok to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Welltok's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xi. requiring Welltok to provide notice to Plaintiffs and all Class Members regarding the full nature and extent of the Data Breach and the disclosure of Private Information to unauthorized persons, including the threat posed as a result of the disclosure of their confidential personal information, and educating Plaintiffs and Class Members regarding steps affected individuals should take to protect themselves;

xii. requiring Welltok to implement logging and monitoring programs sufficient to track traffic to and from Welltok's servers;

xiii. requiring, for a period of 10 years, the appointment of a qualified and independent third-party assessor to conduct an annual SOC 2 Type 2 attestation to evaluate Welltok's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Classes, and to report any deficiencies with compliance of the Court's final judgment;

xiv. requiring Welltok to implement multi-factor authentication requirements, if not already implemented; and

xv. requiring Welltok employees to employ passwords consistent with best security practices and to change their passwords on a timely and regular basis..

h. Award disgorgement and restitution of all earnings, profits, compensation, and benefits received by Welltok as a result of its unlawful acts;

i. Order Welltok to purchase or provide funds for lifetime credit monitoring and identify theft insurance to Plaintiffs and Class Members;

j. Order Welltok to pay all costs necessary to notice Class Members about the judgment and all costs necessary to administer a court approved claims process.

k. Award Plaintiffs and the Classes pre-judgment and post-judgment interest to the maximum extent allowed by law;

l. Grant Plaintiffs and the Classes leave to amend this complaint to conform to the evidence produced during the course of this case;

m. Award Plaintiffs and the Classes reasonable attorneys' fees, costs, and expenses, as allowable;

n. Where necessary, distribute any monies recovered from Welltok on behalf of Class Members or the general public via fluid recovery or cy pres recovery as applicable to prevent Welltok from retaining benefits of its wrongful conduct;

o. Award Plaintiffs and the Class such other favorable relief as allowable under law or at equity;

p. Award any other and further relief as may be just and proper; and

q. Conduct a trial by jury on all issues so triable.

JURY DEMAND

Plaintiffs demand a trial by jury for all Defendants on all issues so triable.

DATED: December 5, 2024

Respectfully submitted,

HAGENS BERMAN SOBOL SHAPIRO LLP

By: */s/ Kristen A. Johnson*
Kristen A. Johnson (BBO# 667261)
1 Faneuil Hall Square, 5th Floor
Boston, MA 02109
Tel: (617) 482-3700
Fax: (617) 482-3003
kristenj@hbsslaw.com

Plaintiffs' Liaison & Coordinating Counsel

By: */s/ E. Michelle Drake*
E. Michelle Drake
BERGER MONTAGUE, PC
1229 Tyler Street, NE, Suite 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
emdrake@bm.net

By: */s/ Gary F. Lynch*
Gary F. Lynch
LYNCH CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
Gary@lcllp.com

By: */s/ Douglas J. McNamara*
Douglas J. McNamara
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue NW, 5th Floor
Washington, DC 20005
Tel: (202) 408-4600
dmcnamara@cohenmilstein.com

By: */s/ Karen H. Riebel*
Karen H. Riebel
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Avenue S, Suite 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
Fax: (612) 612-339-0981
khriebel@locklaw.com

By: */s/ Charles E. Schaffer*
Charles E. Schaffer
Austin B. Cohen
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Tel: (215) 592-1500
Fax: (215) 592-4663
cshaffer@lfsblaw.com
acohen@lfsblaw.com

Plaintiffs' Lead Counsel

CERTIFICATE OF SERVICE

I hereby certify that, on this date, the foregoing document was filed electronically via the Court's CM/ECF system, which will send notice of the filing to all counsel of record.

Dated: December 6, 2024

/s/ Kristen A. Johnson
Kristen A. Johnson (BBO# 667261)

EXHIBIT A

DEFENDANTS' PROPOSED COMPLAINT TRACKS[23, 24]

PROGRESS SOFTWARE CORPORATION TRACK

- Progress Software Corporation
- Ipswitch, Inc.

DIRECT USERS TRACK

- Allegheny County
- American National Group, LLC d/b/a American National Insurance Company
- American National Insurance Company
- Aristocrat Technologies, Inc.
- AutoZone, Inc.
- Cadence Bank
- CareSource
- Chevron Federal Credit Union

[23] These Proposed Complaint Tracks are as of July 30, 2024. Defendants reserve the right to revise or amend these Tracks and add or remove particular Defendants. Defendants make no admissions, whether factual, legal or otherwise, by providing these Tracks.

[24] As set forth in Defendants' Memorandum in Support of Defendants' Omnibus Motion to Dismiss Pursuant to FED. R. CIV. P. 12(b)(1) (ECF No. 1114-1), there is a category of Defendants that are not Direct Users, Vendors, Vendor Contracting Entities, or Vendor Contracting Entity Customers. This other category includes Defendants that appear to have been named by Plaintiffs in an attempt to add seemingly related corporate parents, subsidiaries, affiliates, or related parties to certain cases. In many instances, these Defendants have been improperly named and bear no relationship to Plaintiffs or the MOVEit Security Event. These Defendants are identified herein in parentheses next to their related Defendant entity (*e.g.*, "Defendant (including Related Entity)."). These Defendants do not waive and expressly reserve all rights and defenses relating to their improper inclusion.

- Delta Dental of California (including Dentegra Insurance Co., Delta Dental Insurance Company, Delta Dental of New York, and Delta Dental of Pennsylvania).[25]
- EMS Management & Consultants, Inc.
- Enstar (US) Inc.
- Franklin Mint Federal Credit Union
- Greater Rochester Independent Practice Association, Inc.
- Johns Hopkins University; Johns Hopkins Health System Corporation
- Medical College of Wisconsin, Inc.
- New York City Department of Education
- Paycom
- TD Ameritrade, Inc.
- The Charles Schwab Corporation
- The Vitality Group
- TSG Interactive US Services Ltd.
- Union Bank & Trust Company
- United Health Group
- United Healthcare Student Resources

[25] Please note, this parenthetical does not include Delta Dental Plans Association, Delta Dental of New Jersey, Delta Dental of Iowa, Delta Dental of Tennessee, Delta Dental of Missouri, or Delta Dental of Washington ("Other Delta Dental Entities"). Per prior correspondence with Plaintiffs' Leadership Committee, these Delta Dental entities are not related to Delta Dental of California (only the entities listed in the parenthetical above the line are subsidiaries or affiliates of DDC). These Other Delta Dental entities are not corporate parents, subsidiaries, predecessors, successors-in-interest, or affiliates to Delta Dental of California in any manner whatsoever, nor are they a direct user, a vendor, a vendor contracting entity, or a vendor contracting entity customer. Thus, they do not fall into any track, and they have no relationship (direct or indirect) with any of the Plaintiffs who have alleged causes of action against them.

- University of Rochester
- Unum Group
- Wayne Bank

VENDORS AND INDIRECTLY IMPACTED ENTITIES TRACK(S)

- Vendor: Alogent Holdings, Inc.
- Vendor: Arietis Health, LLC
    - Vendor Contracting Entity: Anesthesia Consulting & Management, LP
        - Vendor Contracting Entity Customer: North Star Anesthesia of Michigan II, P.C.
        - Vendor Contracting Entity Customer: NorthStar Anesthesia of Missouri, Inc.
- Vendor: CBIZ, Inc.
- Vendor: CLEAResult Consulting
    - Vendor Contracting Entity: NSTAR Electric Co. d/b/a Eversource Energy
- Vendor: Data Media Associates, LLC
- Vendor: Ernst & Young Investment Advisers LLP[26]
    - Vendor Contracting Entity: Bank of America Corporation
- Vendor: EyeMed Vision Care LLC
- Vendor: Financial Institution Service Corp.
    - Vendor Contracting Entity: Homeland Bancshares
- Vendor: Fidelity National Info Systems
    - Vendor Contracting Entity: Not Named as Defendant
        - Vendor Contracting Entity Customer: Pathward, N.A.

[26] Not the correct entity.

- Vendor: International Business Machines Corp.
- Vendor: Kirkland & Ellis
    - Vendor Contracting Entity: Not Named as Defendant
        - Vendor Contracting Entity Customers: Trilogy Home Healthcare NE FL., Inc. and Trilogy Home Healthcare SW FL., Inc. (including CenterWell Home Health Services, LLC and Humana Inc.)
- Vendor: Maximus Federal Services, Inc.
- Vendor: Maximus Health Services, Inc.
- Vendor: Maximus, Inc.
- Vendor: Medical Eye Services, Inc. ("MES Vision")
    - Vendor Contracting Entity: California Physicians' Service d/b/a Blue Shield of California
- Vendor: NASCO (National Account Service Company LLC)
- Vendor: National Student Clearinghouse
    - Vendor Contracting Entity: The Trustees of Columbia University in the City of New York
- Vendor: Nuance Communications Inc.
    - Vendor Contracting Entity: Garrett Regional Medical Center
- Vendor: Paycom
- Vendor: Performance Health Technology Ltd.
- Vendor: Pension Benefit Information
    - Vendor Contracting Entity: Aetna Life Insurance Company
    - Vendor Contracting Entity: American General Life Insurance Co.
    - Vendor Contracting Entity: Athene Annuity and Life Company
    - Vendor Contracting Entity: Berwyn Group, Inc.
    - Vendor Contracting Entity: Corebridge Financial, Inc.
    - Vendor Contracting Entity: F&G Annuities & Life, Inc.

- Vendor Contracting Entity: Fidelity Investments Institutional Operations Company LLC
    - Vendor Contracting Entity Customer: Bank of America Corporation
- Vendor Contracting Entity: Not Named as Defendant
    - Vendor Contracting Entity Customer: Fidelity Life Association
- Vendor Contracting Entity: FMR LLC
- Vendor Contracting Entity: FullScope RMS (f/k/a Disability Reinsurance Management Servs)
    - Vendor Contracting Entity Customer: Reliastar Life Insurance Company
    - Vendor Contracting Entity Customer: Reliastar Life Insurance Company of New York
- Vendor Contracting Entities: Genworth Financial, Inc.; Genworth Life and Annuity Insurance Company; Genworth Life Insurance Company
    - Vendor Contracting Entity Customer: Brighthouse Financial, Inc. (wrongly named as defendant in existing complaint, whereas Brighthouse Life Insurance Company is the entity to which plaintiff is connected)
- Vendor Contracting Entity: Hartford Life and Accident Insurance Company
- Vendor Contracting Entity: Jackson National Life Insurance Company
- Vendor Contracting Entity: Manhattan National Life Insurance Company
- Vendor Contracting Entity: MassMutual Ascend Life Insurance Company
- Vendor Contracting Entities: Milliman, Inc.; Milliman Solutions, LLC
    - Vendor Contracting Entity Customer: CMFG Life Insurance Company
    - Vendor Contracting Entity Customer: Foresters Financial Holding Co.
    - Vendor Contracting Entity Customer: MEMBERS Life Insurance Company
    - Vendor Contracting Entity Customer: The Independent Order of Foresters
- Vendor Contracting Entity: Sun Life and Health Insurance Company (U.S.)
- Vendor Contracting Entity: Talcott Resolution Life Insurance Company (and related entities)

- Vendor Contracting Entity: Teachers Insurance & Annuity Association of America
- Vendor Contracting Entity: The Global Atlantic Financial Group LLC (and related entities)
- Vendor Contracting Entity: The Prudential Insurance Company of America
- Vendor Contracting Entity: Not Named as Defendant
  - Vendor Contracting Entity Customer: Continental Casualty Company
  - Vendor Contracting Entity Customer: Lumico Life Insurance Company
  - Vendor Contracting Entity Customer: Standard Insurance Company (and related entities)
  - Vendor Contracting Entity Customer: Puritan Life Insurance Company of America

- Vendor: Radius Global Solutions
- Vendor: Sovos Compliance, LLC
  - Vendor Contracting Entity: Patelco Federal Credit Union
- Vendor: TMG Health
  - Vendor Contracting Entity: Health Care Service Corporation
- Vendor: Welltok, Inc.; Virgin Pulse, Inc.
  - Vendor Contracting Entity: Baylor Scott & White Health
  - Vendor Contracting Entity: CHI Health - NE
  - Vendor Contracting Entity: Optum, Inc.
  - Vendor Contracting Entity: OSF Healthcare System
  - Vendor Contracting Entity: Premier Health Partners
  - Vendor Contracting Entity: Virginia Mason Franciscan Health
  - Vendor Contracting Entity: Sutter Health
  - Vendor Contracting Entity: Not Named as Defendant
    - Vendor Contracting Entity Customer: Corewell Health East/Beaumont Health

- Vendor: Not Named as Defendant
    - Vendor Contracting Entity: Blue Cross Blue Shield of Massachusetts
- Vendor: Not Named as Defendant
    - Vendor Contracting Entity: Community Trust Bank
- Vendor: Not Named as Defendant
    - Vendor Contracting Entity: MasTec
- Vendor: Not Named as Defendant
    - Vendor Contracting Entity: MidFirst Bank (Midland Financial Co.)
- Vendor: Not Named as Defendant
    - Vendor Contracting Entity: Primis Bank
- Vendor: Not Named as Defendant
    - Vendor Contracting Entity: The Bank of Canton
    - Vendor Contracting Entity: Flagstar Bank, N.A.
- Vendor: Not Named as Defendant
    - Vendor Contracting Entity: Umpqua Bank/Columbia Banking Systems, Inc., d/b/a Umpqua Bank
- Vendor: Not Named as Defendant
    - Vendor Contracting Entity: Valley National Bank
- Vendor: Not Named as Defendant
    - Vendor Contracting Entity: Not Named as Defendant
        - Vendor Contracting Entity Customer: American Multi-Cinema, Inc.; AMC Entertainment Holdings, Inc. (d/b/a AMC Theatres)