UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN RE WAWA, INC. DATA SECURITY LITIGATION	**Case No. 19-6019-GEKP**
	Civil Action
This Document Relates to: Consumer Track	**CONSUMER PLAINTIFFS' CONSOLIDATED CLASS ACTION COMPLAINT**
	JURY TRIAL DEMANDED

TABLE OF CONTENTS

I. INTRODUCTION 1

II. PARTIES 3

A. Plaintiffs 3

1. Delaware Plaintiffs 3

a. Plaintiff April Pierce 3

b. Plaintiff Eric Russell 4

c. Plaintiff Charmissha Tingle 7

2. Florida Plaintiffs 9

a. Plaintiff Marcus McDaniel 9

b. Plaintiff Michael Sussman 11

3. Maryland Plaintiffs 13

a. Plaintiff Kenneth Brulinski 13

b. Plaintiff Nicole Portnoy 14

4. New Jersey Plaintiffs 16

a. Plaintiff Kelly Donnelly Bruno 16

b. Plaintiff Joseph Muller 17

5. Pennsylvania Plaintiffs 20

a. Plaintiff Marisa Graziano 20

b. Plaintiff Nakia Rolling 21

6. Virginia Plaintiff 23

a. Plaintiff Amanda Garthwaite 23

7. District of Columbia Plaintiff 24

a. Plaintiff Tracey Lucas 24

B. Defendant 26

III. JURISDICTION AND VENUE 27

IV. FACTUAL ALLEGATIONS 27

A. Wawa Has a History of Credit Card Data Breaches 30

B. Wawa Was on Notice of a Significant Risk of a Data Breach 31

C. Wawa's Privacy Policy 35

D. Wawa's Data Security Failures 37

1. Wawa Violated the Payment Card Industry Data Security Standards 38

2. Wawa Violated the FTC Act 40

3. Wawa Disregarded Guidance Established by the National Institute of Standards and Technology 43

E. As Many as 30 Million Payment Cards May Have Been Impacted by the Data Breach; Stolen Data Has Been Offered for Sale on the "Dark Web"; and Misuse of the Stolen Data Is Ongoing 44

F. Damages to Class Members 48

i. The Stolen Data is at Risk of Misuse for Years 51

ii. Class Members Face a Risk of Identity Theft Beyond Just Credit and Debit Card Fraud 52

V. CLASS ACTION ALLEGATIONS 54

VI. CAUSES OF ACTION 57

COUNT I
NEGLIGENCE
(On Behalf of the Nationwide Class or, in the Alternative, the State Classes) 57

COUNT II
NEGLIGENCE PER SE
(On Behalf of the Nationwide Class or, in the Alternative, the Delaware, Florida, New Jersey, Pennsylvania, Virginia, and District of Columbia Classes) 61

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class or, in the Alternative, the State Classes).....64

COUNT IV
UNJUST ENRICHMENT
(PLEADING IN THE ALTERNATIVE)
(On Behalf of the Nationwide Class or, in the Alternative, the State Classes).....66

COUNT V
VIOLATIONS OF THE DELAWARE CONSUMER FRAUD ACT
6 Del. Code §§ 2513, et seq.
(On Behalf of Plaintiffs Pierce, Russell, Tingle, and the Delaware Class) 68

COUNT VI
VIOLATIONS OF THE FLORIDA DECEPTIVE AND
UNFAIR TRADE PRACTICES ACT,
Fla. Stat. § 501.201, et seq. ("FDUTPA")
(On Behalf of Plaintiffs McDaniel, Sussman, and the Florida Class) 71

COUNT VII
VIOLATIONS OF THE MARYLAND CONSUMER PROTECTION ACT,
Md. Code Ann. Com. Law § 13-101, et seq.
(On Behalf of Plaintiffs Brulinski, Portnoy, and the Maryland Class).....75

COUNT VIII
VIOLATIONS OF THE NEW JERSEY CONSUMER FRAUD ACT,
N.J. Stat. Ann. §§ 56:8-1, et seq. ("NJCFA")
(On Behalf of Plaintiffs Bruno, Muller, and the New Jersey Class).....79

COUNT IX
VIOLATIONS OF THE PENNSYLVANIA UNFAIR TRADE
PRACTICES AND CONSUMER PROTECTION LAW
73 Pa. Stat. §§ 201-1 to 201-9.2 ("UTPCPL")
(On Behalf of Plaintiffs Graziano, Rolling, and the Pennsylvania Class) 83

COUNT X
VIRGINIA CONSUMER PROTECTION ACT,
Va. Code Ann. §§ 59.1-196, et seq.
(On Behalf of Plaintiff Garthwaite and the Virginia Class) 86

COUNT XI
VIOLATION OF THE VIRGINIA PERSONAL
INFORMATION BREACH NOTIFICATION ACT,
Va. Code. Ann. §§ 18.2-186.6
(On Behalf of Plaintiff Garthwaite and the Virginia Class) 90

COUNT XII
VIOLATION OF THE DISTRICT OF COLUMBIA
CONSUMER PROTECTION PROCEDURES ACT
D.C. Code §§ 28-3901, et seq. ("D.C. CPPA")
(On Behalf of Plaintiff Lucas and the District of Columbia Class).....92

COUNT XIII
VIOLATION OF THE DISTRICT OF COLUMBIA
CONSUMER SECURITY BREACH NOTIFICATION ACT,
D.C. Code §§ 28-3851, et seq.
(On Behalf of Plaintiff Lucas and the District of Columbia Class).....95

VII. RELIEF REQUESTED.....96

VIII. JURY TRIAL DEMAND 97

Plaintiffs Kenneth Brulinski, Kelly Donnelly Bruno, Amanda Garthwaite, Marisa Graziano, Tracey Lucas, Marcus McDaniel, Joseph Muller, April Pierce, Nicole Portnoy, Nakia Rolling, Eric Russell, Michael Sussman, and Charmissha Tingle ("Plaintiffs"), on behalf of themselves and all others similarly situated, bring this class action complaint against Defendant Wawa, Inc. ("Defendant" or "Wawa"). Plaintiffs allege as follows upon personal knowledge as to their own acts and experiences, and upon the investigation of their attorneys as to all other matters.

I. INTRODUCTION

1. This is a data breach class action on behalf of Wawa customers whose credit and debit card information were stolen by cybercriminals as part of a massive cyber-attack on Wawa's payment card environment and systems. The data breach involved transactions at all or most of Wawa's 850 convenience stores (including fuel dispensers) over a nine-month period. Information compromised in the breach included credit and debit card numbers, card expiration dates, and cardholder names ("Card Information"). The fraud exposure window of the breach of Wawa's servers lasted from March 4, 2019 until December 12, 2019 (the "Data Breach").

2. Despite the breach being both subjectively and objectively foreseeable, Wawa failed to implement adequate measures to protect the sensitive, non-public information entrusted to it by its customers. Making matters worse, Wawa announced the breach in the midst of the winter holiday shopping season – leaving many consumers without access to payment cards that had to be canceled as a direct result of Wawa's failure to safeguard Card Information.

3. While Wawa initially attempted to downplay the risks that the breach posed to its customers, it has subsequently acknowledged that there have been reports of "criminal attempts to

sell" the consumer data.[1] As discussed in more detail below, Card Information was deliberately targeted by hackers for the purpose of re-selling it to other wrongdoers on illicit marketplaces on the dark web. Indeed, the stolen Card Information is a valuable commodity to identity thieves.

4. As a result of the Data Breach, many class members have experienced and will continue to experience fraudulent credit and debit card transactions and other fraud related to their accounts. Class members have incurred and will continue to incur out-of-pocket costs to purchase protective measures such as credit monitoring services, credit freezes, and credit reports, and pay bank fees, late fees, or other costs directly or indirectly related to the Data Breach.

5. As discussed in more detail below, all named Plaintiffs have sustained actual, palpable misuse of their payment cards and have suffered other types of injuries and damages as a result of the Data Breach. Plaintiffs and class members have also been exposed to a heightened and imminent risk of fraud and identity theft. In addition to the significant inconvenience the breach has already caused, Plaintiffs and class members must now and in the future closely monitor their financial accounts to guard against fraud. This is a burdensome and time-consuming process.

6. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose payment card information was stolen in the Data Breach. Plaintiffs seek remedies including reimbursement of out-of-pocket losses, compensation for time spent in response to the Data Breach and other types of harm, free credit monitoring and identity theft insurance beyond Wawa's current one-year offer, and injunctive relief involving substantial improvements to Wawa's card payment data security systems.

[1] *See* Wawa Provides Customer Update on Previous Data Security Incident, (2020), https://s3.amazonaws.com/wawa-kentico-prod/wawa/media/misc/jan282020 wawapressreleaseupdatetodec-19datasecurityannouncement_1.pdf (last visited Jul 27, 2020).

II. PARTIES

A. Plaintiffs

1. *Delaware Plaintiffs*

a. Plaintiff April Pierce

7. Plaintiff April Pierce is a resident and citizen of Delaware. She used her debit card on at least twenty occasions at Wawa locations in Delaware and Pennsylvania during the Data Breach period.

8. After using her debit card at Wawa, Plaintiff Pierce experienced fraudulent use of the same card. She used her debit card at Wawa on May 6, 2019 and May 13, 2019, among other dates. Shortly thereafter, on or around May 15, 2019, she tried to use her debit card for an in-store purchase. Her card was unexpectedly declined. She was very embarrassed about the denial because she had no other way to pay for the item she was trying to purchase. She called her bank to inquire about the denial. Her bank stated that her card was frozen due to suspected fraudulent activity. The bank indicated that someone tried to use her debit card at a gas station in Lithonia, Georgia. Plaintiff Pierce disputed the charge. The dispute process was time-consuming and involved follow-up phone calls with the bank. The bank ultimately agreed to block the charge.

9. The bank deactivated her debit card and issued a replacement card. It took approximately three to five days for her new card to arrive. Plaintiff Pierce had no convenient way to access her bank account funds in the meantime. During that time, she could not pay bills online or make card-based purchases. Further, she had to withdraw cash to pay for things while awaiting her new card. This was time-consuming and inconvenient. In order to withdraw cash from an ATM machine, she had to contemporaneously talk with a bank representative on the phone so the bank could temporarily unfreeze her card to allow her to withdraw cash, and then re-freeze the card after the ATM transaction was complete. She had to drive approximately five miles (ten miles round

trip) to the ATM machine, which caused her to use gas for her car, an out of pocket loss that she otherwise would not have incurred but for the Data Breach.

10. Plaintiff Pierce also spent time resetting several electronic payment links to her new debit card when it arrived.

11. As a precaution, Plaintiff Pierce placed a credit freeze on her credit report to prevent potential identity theft. This was time-consuming and burdensome.

12. To her knowledge, Plaintiff Pierce had never experienced fraudulent charges on her debit card prior to the Wawa Data Breach.

13. To her knowledge, she has not received any notices from other entities stating that her debit card number was stolen in a data breach. To the best of her knowledge, there are no obvious sources of the fraudulent debit card transaction other than the Wawa Data Breach.

14. As a result of the Wawa Data Breach, Plaintiff Pierce now reviews her financial accounts more closely than she otherwise would have. She has also reset some of her passwords as a precaution. This has been time-consuming and burdensome. She has spent approximately twenty hours thus far in response to the Data Breach, including to review her accounts more carefully, address the fraudulent charge, travel to her bank, reset her electronic payment links, place a credit freeze on her credit report, and reset passwords.

15. Had she known that Wawa had inadequate data security, Plaintiff Pierce would not have used her debit card at Wawa.

b. Plaintiff Eric Russell

16. Plaintiff Eric Russell is a resident and citizen of Delaware. He used his primary credit card on approximately a weekly basis at several Wawa locations in Delaware throughout the Data Breach period. He also used a separate debit card and a second credit card at Wawa

locations in Delaware during the Data Breach period. He used his cards at Wawa locations in at least Newark, DE, Middletown, DE, Wilmington, DE, and Smyrna, DE.

17. After using each of his three payment cards at Wawa, he experienced fraudulent charges on all three of those cards.

18. With respect to Plaintiff Russell's primary credit card, which he typically used at Wawa weekly, one such Wawa purchase took place on September 17, 2019. The next day, on September 18, 2019, fraudulent charges were incurred on the card for $150.00 and $50.00 at "Giant Fuel" in Harrisburg, Pennsylvania. He disputed the fraudulent charges with his bank. This was a time-consuming process. The bank ultimately agreed to reverse the charges.

19. The bank cancelled Plaintiff Russell's credit card and issued a replacement card. However, it took approximately two weeks for the new card to arrive. He did not have access to his credit line during that period.

20. When his new credit card arrived, Plaintiff Russell spent time resetting several electronic payment links to the new card number.

21. With respect to his debit card, he used that card at Wawa on at least June 4, 2019 and June 21, 2019. On November 26, 2019, a $13.99 fraudulent charge was incurred on the card for a PayPal transaction. He disputed the charge with his bank. The bank ultimately agreed to reverse the charge.

22. With respect to his second credit card, he used the card at Wawa on at least May 11, 2019. He very seldom used that credit card, and he used it at only a very small number of merchants, of which Wawa was one. On or around May 6, 2020, a fraudulent charge was incurred on the card. He disputed the charge with his credit card issuer, and the charge was reversed.

23. These incidents of credit and debit card fraud were highly unusual for Plaintiff Russell. He is unaware of having experienced any credit or debit card fraud prior to the Wawa Data Breach. He is also unaware of any obvious sources of the fraudulent transactions other than the Wawa Data Breach.

24. In addition to credit and debit card fraud, Plaintiff Russell experienced several other types of identity theft. On March 30, 2020, he received a letter from the "GreenSky eCommerce Program" informing him that his application for a "GreenSky eCommerce Loan" had been denied because GreenSky was "unable to verify [your] application information." Plaintiff Russell had never applied for the loan. The loan application was fraudulent.

25. On April 3, 2020, Plaintiff Russell received a letter from Synchrony Bank informing him that his request to open a Lowe's credit line was denied because he already has a credit line with Lowe's. Plaintiff Russell did not apply for the new credit line. He already had a Lowe's credit line, which he opened several years earlier. The new credit line application was fraudulent.

26. In April 2020, Plaintiff Russell received a fraudulent Raymour & Flanigan credit card in the mail. The card was issued in his name and had an $8,000 credit limit. He did not apply for the card. He disputed having applied for the account, and he closed it before any charges were incurred.

27. These incidents of identity theft were highly unusual for Plaintiff Russell. He is not aware of having experienced identity theft prior to the Wawa Data Breach. He is unaware of any obvious sources of this identity theft.

28. As a result of this fraudulent credit and debit card activity and identity theft, Plaintiff Russell purchased credit monitoring coverage from "Identity Guard" on April 8, 2020.

The service costs $27.99 per month. He made the first of his monthly payments on April 8, 2020, and he has continued to make monthly payments thereafter.

29. As an additional protective measure, Plaintiff Russell placed a credit freeze on his credit report. He also obtained and reviewed a copy of his credit report. These were time-consuming and burdensome tasks.

30. As a result of the Wawa Data Breach, Plaintiff Russell now reviews his financial accounts more closely than he otherwise would have. It has been a very time-consuming process. Due to the Wawa Data Breach, he has spent many hours reviewing his accounts in detail, investigating and disputing the fraudulent items, and taking the various protective measures noted above.

31. Had he known that Wawa had inadequate data security, Plaintiff Russell would not have used his credit or debit cards at Wawa.

c. Plaintiff Charmissha Tingle

32. Plaintiff Charmissha Tingle is a resident and citizen of Delaware. She used her debit card on an almost weekly basis at Wawa locations in Delaware and Pennsylvania throughout the Data Breach period.

33. After using her debit card at Wawa, Plaintiff Tingle experienced fraudulent charges on the card. Specifically, on October 15, 2019, Plaintiff Tingle experienced four separate fraudulent charges at various locations in California. Three of the charges were at three restaurants in San Gabriel, California for $50.38, $61.90, and $46.25. One charge was at an animal hospital in nearby Rosemead, California for $178.55. All of these fraudulent charges took place just two days after one of Plaintiff Tingle's Wawa purchases.

34. Plaintiff Tingle noticed the fraudulent charges when she checked her account balance and saw that it was significantly lower than she expected. She immediately contacted her

bank to dispute the transactions. The fraudulent transactions were eventually reversed, but not until two weeks later on October 29, 2019. During those two weeks, she was without the use of the funds that were stolen from her account due to the Data Breach. The lack of access to the stolen funds was burdensome and inconvenient.

35. Plaintiff Tingle's car payment was automatically drawn from the same account that was compromised by the Data Breach. However, as a result of the fraudulent transactions on her debit card and diminished funds in that account, the car payment was not processed. She had to explain the situation to her car payment finance company and request an extension. The finance company imposed a $70 late fee, which she paid. That fee would not have been imposed had the Data Breach not resulted in fraudulent charges on her card.

36. Plaintiff Tingle's card issuer cancelled her debit card and issued her a replacement card. However, the replacement card did not arrive until four weeks later. During those four weeks, Plaintiff Tingle had very limited access to her account or the funds in it. Her card issuer is an online-only institution with no brick-and-mortar locations from which to withdraw cash without a debit card. Thus, as a direct and proximate result of the Data Breach, Plaintiff Tingle effectively lost access to her account for a month. Her card issuer charges a $5.00 recurring monthly fee for the account. Although she did not use the account for a month, she was charged the $5.00 fee for that month. Thus, as a direct result of the Data Breach, Plaintiff Tingle suffered a $5.00 out of pocket loss because she paid for an account she could not conveniently access, and did not access, during that month.

37. The loss of use of her account was a major inconvenience to Plaintiff Tingle. The account was her only financial account. In light of the lengthy delay in receiving a replacement card, she had to open a new bank account with a different financial institution. Until she found

time outside of work to go to the new bank and open a new account, she had to temporarily use her fiancée's account because she did not have a functioning bank account of her own. This was a significant burden. Among other things, she had to deposit her paycheck into his account because otherwise she could not quickly or conveniently access the funds from her paycheck.

38. Plaintiff Tingle also spent time resetting several electronic payment links to her new debit card.

39. Prior to these fraudulent debit card charges, to her knowledge, Plaintiff Tingle never experienced fraudulent activity on her debit card account.

40. To her knowledge, Plaintiff Tingle has not received any notices from other entities stating that her debit card number was stolen in a data breach. To the best of her knowledge, there are no obvious sources of the fraudulent activity on her debit card other than the Wawa Data Breach.

41. As a result of the Wawa Data Breach, Plaintiff Tingle now reviews her financial accounts more closely than she otherwise would have. This has been time-consuming and burdensome. She has spent at least ten hours responding to the Data Breach, including reviewing her accounts more carefully, disputing the fraudulent charges, contacting her car payment company, opening a new bank account, and resetting her payment links.

42. Had she known that Wawa had inadequate data security, Plaintiff Tingle would not have used her debit card at Wawa.

2. *Florida Plaintiffs*

a. Plaintiff Marcus McDaniel

43. Plaintiff Marcus McDaniel is a resident and citizen of Florida. He used his debit card at a Wawa location in Florida on at least one occasion during the Data Breach period.

44. After using his debit card at Wawa, Plaintiff McDaniel experienced fraudulent charges on the same card. Specifically, he used his debit card for a Wawa purchase on December 9, 2019. Four days later, on December 13, 2019, fraudulent charges were incurred on his card for $1.60, $4.20, $1.10, and $2.10, each of which was at an entity described on his bank statement as "USA Technology." Two days later, on December 16, 2019, additional fraudulent charges were incurred on the same card for $99.90 at "Gate 1143," and $100.00 at "ExxonMobil."

45. Plaintiff McDaniel disputed all six fraudulent charges with his bank. The dispute process involved several phone calls to his bank, including calls that Plaintiff McDaniel made while he was at work. He had to call multiple times because the bank could not fully investigate or reverse the charges until each individual charge cleared the bank and was posted to his account. When the charges did clear the bank, they cleared on different days (four charges on one day and two charges on another day), and at different times during the day. Plaintiff McDaniel monitored his account online and called the bank as soon as each charge cleared the bank. On each call he had to re-explain the entire situation to the customer service representative, which was a different person each time. As a result of his efforts, his bank ultimately reversed the fraudulent charges.

46. The bank cancelled Plaintiff McDaniel's debit card and issued a replacement card. However, the process took several days, and Plaintiff McDaniel had no convenient way to access his bank account in the interim. This was particularly inconvenient because the card replacement process occurred during the holiday shopping season. Moreover, Plaintiff McDaniel had to drive to his bank to pick up his replacement card in-person, which caused him to incur out of pocket costs for gas for his car that he would not have incurred but for the Data Breach.

47. Plaintiff McDaniel also spent time resetting several electronic payment links to his new debit card when it arrived.

48. To his knowledge, Plaintiff McDaniel never experienced any fraudulent charges on his debit card or bank account prior to the Wawa breach.

49. To his knowledge, Plaintiff McDaniel has not received any notices from other entities stating that his debit card number was stolen in a data breach. To the best of his knowledge, there are no obvious sources of the fraudulent activity on his debit card other than the Wawa Data Breach.

50. As a result of the Wawa Data Breach, Plaintiff McDaniel now reviews his financial accounts more closely than he otherwise would have. This has been time-consuming and burdensome. Plaintiff McDaniel has spent at least fifteen to twenty hours responding to the Data Breach, including reviewing his accounts more carefully, investigating and disputing the fraudulent charges with his bank, traveling to the bank to pick up his replacement card, and resetting his electronic payment links.

51. Had he known that Wawa had inadequate data security, Plaintiff McDaniel would not have used his debit card at Wawa.

b. Plaintiff Michael Sussman

52. Plaintiff Michael Sussman is a resident and citizen of Florida. He used his credit card at least ten to fifteen times at multiple Wawa locations throughout Florida during the Data Breach period.

53. After using his credit card at Wawa, Plaintiff Sussman experienced a fraudulent charge on the same card. On December 4, 2019, his credit card issuer alerted him by email to fraudulent activity on the card. A fraudulent charge for $924.14 was made at a Walmart Supercenter. Plaintiff Sussman immediately called the issuer to gather more information. Refraining from disclosing the exact source of the data breach that led to the fraud, the representative did comment that many of the company's cardholders had increased fraud incidents

during that same week. The credit card company reversed the fraudulent charge on Plaintiff Sussman's account.

54. The card issuer canceled Plaintiff Sussman's credit card and issued a replacement card. The new card was not available for three to four days. Plaintiff Sussman had no convenient way to access his credit line during that period of time. This was particularly inconvenient and burdensome because this was Plaintiff Sussman's primary credit card account. He had to forego a business meeting and related travel due to the temporary unavailability of the card.

55. To his knowledge, Plaintiff Sussman has not received any notices from other entities stating that his credit card number was stolen in a data breach. To the best of his knowledge, there are no obvious sources of the fraudulent transaction other than the Wawa Data Breach.

56. In response to the fraudulent activity, Plaintiff Sussman purchased a copy of his Experian credit report in January 2020 at a cost of $20. He purchased another copy of his credit report in March 2020, again paying $20.

57. In further response to the fraudulent activity, Plaintiff Sussman purchased credit monitoring services from Buildworth Strategies, a local credit repair agency. The cost of the service is $89.99 per month. He has been paying the $89.99 fee each month since January 2020. He also paid a $150 enrollment fee when signing up with Buildworth.

58. Plaintiff Sussman also took unpaid time off from his job to deal with the credit card fraud and his Buildworth Strategies credit monitoring service.

59. As a result of the Wawa Data Breach, Plaintiff Sussman now reviews his financial accounts more closely than he otherwise would have. He also had to forward notarized identity statements to his credit monitoring service provider, Buildworth Strategies, in order to reestablish his correct identity after it had been compromised as result of the Data Breach. This has been time-

consuming and burdensome. He has already expended a significant amount of time in response to the Data Breach, including to review his accounts more carefully, dispute the fraudulent credit card charge, and sign up for and oversee his credit monitoring service.

60. Had he known that Wawa had inadequate data security, Plaintiff Sussman would not have used his credit card at Wawa.

3. *Maryland Plaintiffs*

a. Plaintiff Kenneth Brulinski

61. Plaintiff Kenneth Brulinski is a resident and citizen of Maryland. He used his debit card on approximately a weekly basis at multiple Wawa locations in Maryland throughout the Data Breach period.

62. After Plaintiff Brulinski used his debit card at Wawa, fraudulent transactions were posted to the same debit card account. One particular purchase he made at Wawa took place on November 14, 2019. On that same day, fraudulent charges of $44.99 and $67.93 were incurred on the card at Hulu, a television streaming website. Two weeks later, on November 27, 2019, fraudulent charges of $6.99 and $6.99 were incurred on the card for transactions described as "Google * Little Bird Internet." He disputed the fraudulent charges with his bank, which was a time-consuming process. As a result of his efforts, the bank ultimately reversed the charges.

63. The bank also cancelled Plaintiff Brulinski's debit card and issued him a new one. However, it took approximately seven days for the new card to arrive. Plaintiff Brulinski had no convenient way to access his bank account funds in the meantime, and could not conveniently pay bills or make purchases during that time period. He had to drive to his bank twice during that period to withdraw cash in-person, which was a time-consuming and inconvenient process. The trips consumed gas for his car, which was an out of pocket cost that Plaintiff Brulinski otherwise would not have incurred but for the Data Breach.

64. Plaintiff Brulinski also spent time resetting several electronic payment links to his new debit card when it arrived.

65. To his knowledge, Plaintiff Brulinski had never experienced fraudulent charges on his debit card or bank account prior to the Wawa breach.

66. To his knowledge, Plaintiff Brulinski has not received any notices from other entities stating that his debit card number was stolen in a data breach. To the best of his knowledge, there are no obvious sources of the fraudulent debit card transactions other than the Wawa Data Breach.

67. As a result of the Wawa Data Breach, Plaintiff Brulinski now reviews his financial accounts more closely than he otherwise would have, and he has reset many of his passwords. This has been time-consuming and burdensome. He has spent several hours thus far in response to the Data Breach, including to review his accounts more carefully, investigate and dispute the fraudulent charges with his bank, travel to the bank to withdraw cash, and reset his electronic payment links.

68. Had he known that Wawa had inadequate data security, Plaintiff Brulinski would not have used his debit card at Wawa.

b. Plaintiff Nicole Portnoy

69. Plaintiff Nicole Portnoy is a resident and citizen of Maryland. She used her debit card on at least twelve occasions at Wawa locations in Maryland and Pennsylvania throughout the Data Breach period. She used her debit card at Wawa locations in Frederick, MD, Dunkirk, MD, Hanover, MD, Halethorpe, MD, Joppa, MD, and Trevose, PA.

70. After using her debit card at Wawa, Plaintiff Portnoy experienced fraudulent charges on the same card. One Wawa purchase took place on November 26, 2019. Later that same day, two fraudulent transactions posted to Plaintiff Portnoy's debit card account. One was a

$963.07 charge incurred at HP's online store, and the other was a $32.00 charge incurred at a Bed Bath & Beyond store in Totowa, New Jersey.

71. Plaintiff Portnoy visited her bank the next day to dispute these charges. Her bank canceled her card and gave her a replacement card that day. To get to the bank, she traveled several miles from her home in Maryland to her bank branch in Pennsylvania. The trip consumed gas for her car, which was an out-of-pocket cost that Plaintiff Portnoy would not have incurred but for the Data Breach. The visit to the bank also caused her to miss a day of work.

72. The fraudulent charges were eventually reversed. However, it took approximately two weeks before the money was restored to Plaintiff Portnoy's account. In the meantime, she lost the use of, and was without the benefit of, those stolen funds. She had to use a credit card to pay her rent and other bills, and she also had to borrow money from her mother. She also notified her apartment management company that her rent payment would be late due to her funds being unavailable from the debit card fraud.

73. Plaintiff Portnoy also spent time changing her debit card information with the vendors that electronically deduct funds from her account for regular bills and expenses.

74. To her knowledge, Plaintiff Portnoy has not received any notices from other entities stating that her debit card number was stolen in a data breach. To the best of her knowledge, there are no obvious sources of the debit card fraud other than the Wawa Data Breach.

75. As a result of the Wawa Data Breach, Plaintiff Portnoy now reviews her financial accounts more closely than she otherwise would have. This has been time-consuming and burdensome. She has spent several hours thus far in response to the Data Breach, including to review her accounts more carefully, travel to and dispute the fraudulent charges with her bank,

reset her electronic payment links, borrow money from her mother, and correspond with her apartment management company.

76. Had she known that Wawa had inadequate data security, Plaintiff Portnoy would not have used her debit card at Wawa.

4. *New Jersey Plaintiffs*

a. Plaintiff Kelly Donnelly Bruno

77. Plaintiff Kelly Donnelly Bruno is a resident and citizen of New Jersey. She used her debit card on a weekly basis at multiple Wawa locations in New Jersey throughout the Data Breach period. She used her debit card at Wawa locations in at least Brunswick, NJ and Bridgewater, NJ.

78. After Plaintiff Bruno used her debit card at Wawa, fraudulent charges were made on that same card. On December 27, 2019, four fraudulent transactions were charged to Ms. Bruno's debit card: (1) two separate charges at Target.com, both in the amount of $96.29; (2) another charge at Target.com in the amount of $90.92; and (3) another charge at Target.com in the amount of $50.00 (which subsequently split into two separate $25 charges at Target.com). Then, on December 30, 2019, Plaintiff Bruno's card incurred another fraudulent charge at Target.com in the amount of $90.92.

79. Plaintiff Bruno discovered the fraudulent charges within a day or two and immediately called her bank to dispute the transactions. As a result of her efforts, the bank agreed to reverse the charges. She also called Target to ask how the fraudulent transactions were made. The Target representative told her they were online purchases, but could not provide any further information.

80. Her bank cancelled Plaintiff Bruno's debit card and issued her a new one. However, it took approximately seven days for her new card to arrive. This was an inconvenience because she had no reasonable means of accessing her account while she was awaiting her new card.

81. To her knowledge, Plaintiff Bruno had never experienced fraudulent charges on her debit card prior to the Wawa breach.

82. To her knowledge, Plaintiff Bruno has not received any notices from other entities stating that her debit card number was stolen in a data breach. To the best of her knowledge, there are no obvious sources of the debit card fraud other than the Wawa Data Breach.

83. As a result of the Wawa Data Breach, Plaintiff Bruno now reviews her financial accounts more closely than she otherwise would have. This has been time-consuming and burdensome. Plaintiff Bruno has spent several hours thus far in response to the Data Breach, including to review her accounts more carefully, dispute the fraudulent charges with her bank, and call Target to inquire about the fraudulent charges.

84. Had she known that Wawa had inadequate data security, Plaintiff Bruno would not have used her debit card at Wawa.

b. Plaintiff Joseph Muller

85. Plaintiff Joseph Muller is a resident and citizen of New Jersey. He used his debit card on dozens of occasions at multiple Wawa locations in New Jersey throughout the Data Breach period.

86. After using his debit card at Wawa, Plaintiff Muller suffered fraudulent charges on the same card on several occasions. One fraudulent charge was incurred in July 2019. He disputed the charge with his bank. The bank reversed the charge. The bank also cancelled his card and issued a replacement card.

87. In response to the fraudulent use of his debit card, Plaintiff Muller purchased a copy of his credit report from Experian for $26.65 on July 17, 2019. The fee he paid was an out of pocket cost that he would not have incurred but for the Wawa Data Breach. He reviewed his credit report as a precaution to search for any fraudulent or suspicious items.

88. Plaintiff Muller used his replacement debit card at Wawa on many occasions. After doing so, he suffered a fraudulent charge on the replacement card. Specifically, in or around September 2019, a fraudulent charge was incurred on the card for approximately $60. Plaintiff Muller disputed the charge with his bank. The bank reversed the charge. The bank also cancelled his replacement card and issued a second replacement card.

89. Plaintiff Muller used his second replacement debit card at Wawa on many occasions. After doing so, he suffered yet another fraudulent charge. Specifically, on December 6, 2019, a fraudulent charge was incurred on his second replacement card for $400.00. He disputed the charge with his bank. The bank reversed the charge. The bank also cancelled his second replacement debit card and issued a third replacement card.

90. Each time his debit card was cancelled and reissued, Plaintiff Muller had to wait approximately seven to ten days for the new debit card. Plaintiff Muller had no convenient way to access his bank account funds while awaiting each replacement card. On two separate occasions, he had to drive to his bank to pick up his new debit card in-person. On both occasions he had to drive approximately 40 miles round trip because his bank branch is not located near his house. The lengthy trips consumed gas for his car, which was an out of pocket cost that Plaintiff Muller would not have incurred but for the Data Breach. The trips to the bank took approximately one hour and fifteen minutes each round trip, which was a substantial inconvenience.

91. Each time he received a new replacement debit card, Plaintiff Muller spent time re-establishing five to ten payment links to the new card. This was a time-consuming and burdensome process.

92. To his knowledge, Plaintiff Muller has not received any notices from other entities stating that his debit card number was stolen in a data breach. To the best of his knowledge, there are no obvious sources of the debit card fraud other than the Wawa Data Breach. Plaintiff Muller's purchases at Wawa were a common link to each of his three successive debit cards that experienced fraudulent activity.

93. Separately, Plaintiff Muller also used a credit card at Wawa on many occasions throughout the Data Breach period. The credit card was issued by a bank other than the bank that issued his debit card. After using his credit card at Wawa, Plaintiff Muller experienced fraud on the same credit card. Specifically, on May 1, 2019, a fraudulent charge was incurred on his card for $106.00 at Target. The next day, on May 2, 2019, two more fraudulent charges were incurred at Target for $100.00 and $50.00. Plaintiff Muller disputed the fraudulent charges with his credit card issuer. The card issuer agreed to reverse the charges. The credit card company also cancelled the card and issued a replacement card.

94. To his knowledge, Plaintiff Muller has not received any notices from other entities stating that his credit card number was stolen in a data breach. To the best of his knowledge, there are no obvious sources of the credit card fraud other than the Wawa Data Breach.

95. As a result of the Wawa Data Breach, Plaintiff Muller now reviews his financial accounts more closely than he otherwise would have. This has been time-consuming and burdensome. He has spent at least ten to fifteen hours thus far in response to the Data Breach, including to review his accounts more carefully, investigate and dispute the fraudulent charges

with his bank and credit card issuer, travel to his bank to pick up the replacement debit cards, and reset his electronic payment links.

96. Had he known that Wawa had inadequate data security, Plaintiff Muller would not have used his debit card or credit card at Wawa.

5. *Pennsylvania Plaintiffs*

a. Plaintiff Marisa Graziano

97. Plaintiff Marisa Graziano is a resident and citizen of Pennsylvania. She used her debit card on at least ten occasions at multiple Wawa locations in Pennsylvania and Delaware throughout the Data Breach period. She used her card at Wawa locations in at least West Chester, PA, North Wales, PA, and Delmar, DE.

98. After using her debit card at Wawa, Plaintiff Graziano experienced several fraudulent transactions on the same debit card. Specifically, on December 10, 2019, fraudulent charges were incurred on her card for $99.54 and $99.90, both of which were at a Wawa store in Piscataway, New Jersey. Also, on December 13, 2019, fraudulent charges were incurred on her card for $99.42 and $99.55, both of which were at a Wawa store in Rahway, New Jersey. On that same day, December 13, 2019, fraudulent charges were incurred for $99.60 and $99.60 on her card at a "Quick Chek" convenience store in Ramsey, New Jersey.

99. Plaintiff Graziano disputed these fraudulent charges with her bank. The bank ultimately reversed the charges, but did not do so until two weeks later on December 27, 2019. Plaintiff Graziano was without the use or benefit of the stolen funds in the meantime. This was an inconvenience.

100. Plaintiff Graziano's bank cancelled her debit card and issued a replacement card. However, the new card was not available for approximately one week. She had no convenient way to access her bank account funds in the meantime. Further, she had to drive to her bank to pick up

her new debit card in-person. She drove approximately ten miles round trip. The trip consumed gas for her car, which was an out of pocket cost she would not have incurred but for the Data Breach.

101. After receiving her new debit card, Plaintiff Graziano spent a significant amount of time resetting ten to fifteen electronic payment links to her new card number.

102. As a result of the fraudulent debit card transactions, Plaintiff Graziano obtained a copy of her credit report and reviewed it for fraudulent activity. This was a time-consuming and burdensome process.

103. To her knowledge, Plaintiff Graziano had never experienced fraudulent charges on her debit card prior to the Wawa breach. To the best of her knowledge, there are no obvious sources of the fraudulent debit card activity other than the Wawa Data Breach.

104. As a result of the Wawa Data Breach, Plaintiff Graziano now reviews her financial accounts more closely than she otherwise would have. She also reset many of her passwords as a precaution. This has been time-consuming and burdensome. She has spent approximately thirty hours thus far in response to the Data Breach, including reviewing her accounts more carefully, investigating and disputing the fraudulent charges, obtaining a replacement card, resetting electronic payment links, resetting passwords, and obtaining and reviewing her credit report.

105. Had she known that Wawa had inadequate data security, Plaintiff Graziano would not have used her debit card at Wawa.

b. Plaintiff Nakia Rolling

106. Plaintiff Nakia Rolling is a resident and citizen of Pennsylvania. She used her debit card on many occasions at multiple Wawa locations in Pennsylvania throughout the Data Breach period.

107. After using her debit card at Wawa, Plaintiff Rolling experienced a fraudulent charge on the same card. Specifically, on November 29, 2019, her debit card was used to make a fraudulent card-based purchase on eBay for $322.29. She contacted her bank that same day to dispute the charge. The bank ultimately reversed the charge. However, it did not do so for approximately seven to ten days. During that time, Plaintiff Rolling was without the benefit or use of the funds used to make the fraudulent charge.

108. Her bank cancelled her debit card and reissued a replacement card. However, it took approximately seven days before she received her new card in the mail. During that time, Plaintiff Rolling was without the benefit of using her primary debit card, and she had to visit her bank in-person to transfer funds to another card so she could conduct everyday transactions and holiday shopping. As a result of the loss of use of her card and the temporary loss of the stolen $322.29 while the fraud was being investigated, Plaintiff Rolling was significantly inconvenienced.

109. Plaintiff Rolling also spent a significant amount of time resetting electronic payment links with every vendor that automatically deducts bills and expenses from her debit card.

110. Plaintiff Rolling regularly monitors her credit profile using a service from Capital One called CreditWise. After discovering the fraudulent charges on her debit card, she checked her credit on CreditWise and was informed that her email address was found on the "dark web" on November 30, 2019. In response, she contacted Experian and Equifax to set up fraud alerts on her credit report. This was a time-consuming and burdensome course of events.

111. To her knowledge, Plaintiff Rolling had never experienced fraudulent charges on her debit card or bank account prior to the Wawa breach.

112. To her knowledge, Plaintiff Rolling has not received any notices from other entities stating that her debit card number was stolen in a data breach. To the best of her knowledge, there are no obvious sources of the fraudulent debit card transactions other than the Wawa Data Breach.

113. As a result of the Wawa Data Breach, Plaintiff Rolling now reviews her financial accounts more closely than she otherwise would have. This has been time-consuming and burdensome. She has spent at least three to five hours thus far in response to the Data Breach, including to review her accounts more carefully, investigate and dispute the fraudulent charge, travel to her bank, reset her electronic payment links, check her credit, and set up the fraud alerts.

114. Had she known that Wawa had inadequate data security, Plaintiff Rolling would not have used her debit card at Wawa.

6. *Virginia Plaintiff*

a. Plaintiff Amanda Garthwaite

115. Plaintiff Amanda Garthwaite is a resident and citizen of Virginia. She used her debit card at a Wawa location in Warrenton, Virginia on at least one occasion during the Data Breach period.

116. After using her debit card at Wawa, Plaintiff Garthwaite experienced fraudulent charges on the same card. She used her debit card at Wawa on August 29, 2019. Thereafter, in November 2019, her debit card incurred two fraudulent charges, one for approximately $2,000 at a merchant called Zumiez, and the other at Walmart. Her bank alerted her to the fraudulent charges. She responded to the alert and disputed the transactions. As a result, her bank was able to block the charges before they went through.

117. The bank also cancelled Plaintiff Garthwaite's debit card and issued a replacement card. It took approximately five days for the new card to arrive. This was an inconvenience because she had no other payment cards to use while awaiting the replacement card.

118. Plaintiff Garthwaite also spent time resetting several electronic payment links to her new debit card when it arrived.

119. To her knowledge, Plaintiff Garthwaite had never experienced fraudulent charges on her debit card prior to the Wawa Data Breach.

120. To her knowledge, Plaintiff Garthwaite has not received any notices from other entities stating that her debit card number was stolen in a data breach. To the best of her knowledge, there are no obvious sources of the fraudulent debit card transactions other than the Wawa Data Breach.

121. As a result of the Wawa Data Breach, Plaintiff Garthwaite now reviews her financial accounts more closely than she otherwise would have. She has also reset some of her passwords as a precaution. This has been time-consuming and burdensome. She has spent at least two hours thus far in response to the Data Breach, including to review her accounts more carefully, address the fraudulent charge, reset her payment links, and reset passwords.

122. Had she known that Wawa had inadequate data security, Plaintiff Garthwaite would not have used her debit card at Wawa.

7. *District of Columbia Plaintiff*

a. Plaintiff Tracey Lucas

123. Plaintiff Tracey Lucas is a resident and citizen of the District of Columbia. She used debit cards on several occasions at Wawa locations in the District of Columbia and Maryland during the Data Breach period.

124. After using two different cards at Wawa, Plaintiff Lucas experienced fraudulent charges on both cards.

125. On or around July 13, 2019, Plaintiff Lucas experienced several fraudulent charges on her first debit card. One charge was for a $400 online transaction at T-Mobile. There were other

fraudulent transactions on the same debit card on or around that same date. She contacted her bank to dispute the fraudulent charges. The bank agreed to reverse the charges. The bank also canceled her debit card, closed her account, opened a new account, and issued a new debit card.

126. After using her new debit card at Wawa, Plaintiff Lucas experienced another fraudulent charge. In November 2019, a $14 fraudulent charge was incurred on her new debit card for an iTunes transaction. She disputed the charge with her bank. The bank agreed to reverse it. The bank also cancelled the debit card and issued a replacement card.

127. Both times that her debit cards incurred fraudulent charges and were cancelled and reissued by her bank, Plaintiff Lucas was highly inconvenienced. It took approximately seven to ten days, each time, to receive a reissued card. During those separate seven-to-ten-day periods without a debit card, Plaintiff Lucas did not have convenient access to the funds in her bank account. As a result, she had to drive to her bank to withdraw cash while she was without the use of her cards. She did this on three or four separate occasions. On each occasion, her trip to the bank took one to two hours because she lives in the District of Columbia and her bank is located in Virginia. The trips to the bank also consumed gas for her car, which was an out of pocket cost that Plaintiff Lucas would not have incurred had her debit cards not been compromised by the Data Breach.

128. As a direct result of the fraudulent activity and disruption to her debit card account, Plaintiff Lucas was late paying her cable bill. Her cable company charged her a late fee, which she had to pay. She paid the late fee, and it was not subsequently reversed.

129. Separately, Plaintiff Lucas used another debit card at Wawa during the Data Breach period, on March 15, 2019. She subsequently experienced fraudulent activity on that card, consisting of a series of fraudulent card-based iTunes transactions on June 3, 2019 for $1.37, on

June 8, 2019 for $11.63, on August 1, 2019 for $10.59, on August 30, 2019 for $2.11, on September 27, 2019 for $5.29, and on October 10, 2019 for $12.70. She disputed these charges with her card issuer, and the charges were reversed. The card issuer cancelled her card and issued her a replacement card. She had no access to her funds while the replacement card was pending. Plaintiff Lucas suffered inconvenience as a result.

130. To her knowledge, Plaintiff Lucas had never experienced fraudulent charges on either of her debit cards prior to the Wawa Data Breach.

131. To her knowledge, Plaintiff Lucas has not received any notices from other entities stating that her debit card numbers were stolen in a data breach.

132. As a result of the Wawa Data Breach, Plaintiff Lucas now reviews her financial accounts more closely than she otherwise would have. She has also reset some of her passwords as a precaution. This has been time-consuming and burdensome. She has spent at least ten hours thus far in response to the Data Breach, including to review her accounts more carefully, investigate and dispute the fraudulent charges, and change her passwords. This is in addition to the several hours spent driving to her bank to withdraw cash on multiple occasions.

133. Had she known that Wawa had inadequate data security, Plaintiff Lucas would not have used her debit cards at Wawa.

B. Defendant

134. Wawa, Inc. is a privately held company with its principal place of business in Wawa, Pennsylvania. It is incorporated in New Jersey. It operates more than 850 convenience stores in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida, and the District of

Columbia. Wawa is one of the largest privately-owned companies in the United States.[2] It employs over 35,000 individuals and it reportedly generated revenue of over $12 billion in 2019.

III. JURISDICTION AND VENUE

135. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5 million, and many members of the class are citizens of states different from Wawa.

136. This Court has personal jurisdiction over Wawa because it is headquartered in this district, is registered and regularly conducts business in Pennsylvania, has sufficient minimum contacts in Pennsylvania such that Wawa intentionally avails itself of this Court's jurisdiction by conducting operations here and contracting with companies in this District, and the wrongful acts alleged in the Complaint were committed largely in Pennsylvania.

137. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to Plaintiffs' claims occurred in this District. Venue is also proper pursuant to 28 U.S.C. § 1391(b)(1) because Wawa is headquartered in this District, and is a resident for venue purposes because it regularly transacts business here. Furthermore, Wawa is subject to personal jurisdiction in this District.

IV. FACTUAL ALLEGATIONS

138. Wawa is a chain of convenience stores and fuel dispensers operating on the east coast of the United States (largely the Mid-Atlantic region). It was founded in 1803 as an iron foundry in New Jersey. In 1890 the company was relocated to Delaware County, Pennsylvania where Wawa began operations as a dairy farm.

---

[2] *See* FORBES, *America's Largest Private Companies*, https://www.forbes.com/companies/wawa/?list=largest-private-companies#5aeaad572644 (last visited July 24, 2020).

139. As of 2020, Wawa owns and operates approximately 850 locations in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, the District of Columbia, and Florida. It is the largest convenience store chain in the Greater Philadelphia area, and it is also the third-largest retailer of food in this region. Wawa's locations consist of two types of storefronts: the traditional Wawa convenience store, and "Super Wawa" locations, which are convenience stores that have fuel dispensers. According to Forbes, Wawa was the 25th largest privately held company in the United States in 2018.[3]

140. On December 19, 2019, Wawa CEO Chris Gheysens publicly announced and acknowledged the Data Breach in an open letter entitled "Notice of Data Breach" that was posted on the Wawa website.[4] The letter provided the following:

> Wawa has experienced a data security incident. Our information security team discovered **malware on Wawa payment processing servers** on December 10, 2019, and contained it by December 12, 2019. This malware affected customer payment card information used at **potentially all Wawa locations** beginning at different points in time after March 4, 2019 and until it was contained ….
>
> * * *
>
> Based on our investigation to date, we understand that at different points in time after March 4, 2019, malware began running on in-store payment processing systems at potentially all Wawa locations. Although the dates may vary and some Wawa locations may not have been affected at all, this malware was present on most store systems by approximately April 22, 2019. Our information security team identified this malware on December 10, 2019, and by December 12, 2019, they had blocked and contained this malware ….
>
> * * *
>
> Based on our investigation to date, this malware affected payment card information, including **credit and debit card numbers, expiration dates, and cardholder names on payment cards used at potentially all Wawa in-store payment terminals and fuel dispensers beginning at different points in time after March 4, 2019 and ending on December 12, 2019**. Most locations were affected as of

[3] *See supra*, note 2.

[4] *See Wawa Notifies Customers of Data Security Incident (12/19/2019) Press Release,* Wawa Data Security Incident (Dec. 19. 2019), https://www.wawa.com/alerts/data-security.

> April 22, 2019, however, some locations may not have been affected at all. No other personal information was accessed by this malware ….[5]

141. Mr. Gheysen's letter acknowledged that **Wawa did not discover the Data Breach for over nine months after hackers initially infiltrated Wawa's systems**, and that Wawa did not publicly disclose the Data Breach for over a week after discovering it.

142. Wawa stated that it believes the "malware no longer poses a risk to customers using payment cards at Wawa."[6] However, that assessment does not account for the possibility that Wawa customers whose data has been stolen have been or will be victimized by fraud and/or identity theft resulting from the Data Breach.

143. Wawa also noted that the malware "may have captured some information about Wawa gift card numbers."[7]

144. Wawa claimed that CVV2 numbers (the three or four-digit security code printed on the back of credit and debit cards) were not stolen in the breach.[8] However, CVV2 numbers for the stolen cards reportedly are available for sale on the "dark web," an underground or "black market" part of the internet accessed by an anonymizing browser and not indexed by search engines, where rampant illegal commerce occurs (*e.g.*, buying and selling stolen card, subscription, and account information/credentials), as discussed more fully below. In any event, even if the CVV2 numbers were not stolen, thieves can still make fraudulent transactions without access to those numbers:

> [T]hree- or four-digit security codes weren't stolen, but that doesn't necessarily matter for the hackers, per [data security expert Matthew] Wilson. A three-digit

---

[5] *Id*. (emphasis added).
[6] *See id.*
[7] *Frequently Asked Questions*, Wawa Data Security Incident (Dec. 19, 2019), https://www.wawa.com/alerts/data-security.
[8] *See supra*, note 4.

> code has only 999 possible answers, after all. "That sounds like lot to human," he says. "To a machine, it's nothing."[9]

145. Indeed, fifteen state attorneys general, including the Pennsylvania Attorney General, have confirmed that identity thieves can commit credit or debit card fraud without using CVV2 numbers.[10]

146. Wawa had a duty pursuant to common law, industry standards, payment card network rules, and representations made in its own privacy policy to keep consumers' Card Information confidential and to protect it from unauthorized access.

147. Wawa failed to properly safeguard class members' Card Information, allowing cybercriminals to access the credit and debit Card Information for nine months undetected. The length of the Data Breach demonstrates that Wawa also had faulty network monitoring procedures in place. Had Wawa properly monitored its card payment systems, it would have discovered the malware and siphoning of massive amounts of data much sooner than nine months after the breach began.

A. Wawa Has a History of Credit Card Data Breaches

148. Wawa has a history of credit card intrusions. In 2013, Wawa customers suffered credit card fraud tied to the theft of card information from one of its convenience stores:

> Customers who shopped at a Wawa on Salem Road in Burlington, New Jersey noticed fraudulent purchases on their credit cards. Investigators were able to trace the fraud to four people and arrest them. The four men were charged with credit card theft, credit card fraud, identity theft, and having electronic devices for criminal use. More victims are expected to be found.[11]

---

[9] David Murrell, *The Wawa Credit Card Breach: What You Need to Know*, PHILADELPHIA MAGAZINE (Dec. 20, 2019), https://www.phillymag.com/news/2019/12/20/wawa-data-breach/.
[10] Eric T. Schneiderman, Joint Letter, RE: Aptos Communications with Client-Retailers Resulting from Data Breach (June 5, 2017) (noting that "some of the most popular websites do not require a CVV code to make a purchase"), https://www.law360.com/articles/934951/attachments/0.
[11] Privacy Rights Clearinghouse, Excel Spreadsheet Describing Data Breaches, https://privacyrights.org/data-breaches (last visited July 22, 2020).

149. More recently, in 2018, police investigated a skimming device placed on a Wawa fuel dispenser, which reportedly led to fraudulent credit card transactions.[12]

150. These breaches, coupled with countless others throughout the retail industry, put Wawa and its data security team on notice of the importance of data security, the fact that thieves were aggressively seeking stolen credit card information from Wawa, and the harm that could result from weak data security. Despite these events, Wawa failed to adopt adequate data security governing its credit and debit card transactions.

B. Wawa Was on Notice of a Significant Risk of a Data Breach

151. Wawa was well aware of its data security obligations given the substantial increase in payment card data breaches throughout the retail industry preceding the Data Breach, including numerous recent malware-based payment card breaches. The increase in data breaches and the risk of future breaches was widely known throughout the retail industry, including to Wawa. For instance, Experian reported that 14.2 million Americans had their credit card numbers stolen in 2017, an 88% increase in the amount of credit cards numbers stolen in the United States from 2016.[13]

152. Data security experts have warned since as early as February 2016 that convenience store and gas station chains like Wawa appear to be most susceptible to data breaches, according to a study titled "Data Breach QuickView: 2015 Data Breach Trends," from the Virginia-based Risk Based Security.[14] Risk Based Security's Chief Executive Officer, Barry Kouns, explained

[12] Logan Krum, *Police Investigating Credit Fraud Related to Wawa*, NORTHEAST TIMES (May 24, 2018), https://northeasttimes.com/2018/05/24/police-investigating-credit-fraud-related-to-wawa/.
[13] *See* Matt Tatham, *Identity Theft Statistics*, EXPERIAN (Mar. 15, 2018), https://www.experian.com/blogs/ask-experian/identity-theft-statistics.
[14] *See* Roy Urrico, *Breaches Infest C-Stores, Gas Stations: Study*, CREDIT UNION TIMES (Feb. 9, 2016, 1:09 PM), https://www.cutimes.com/2016/02/09/breaches-infest-c-stores-gas-stations-.study/?slreturn=20200601112550.

that "[t]he fragmented nature of the retail convenience store and gas station business and the ease of accessing pumps not visible to cashiers encourage multiple breaches."

153. In the data breach universe, malware-related data breaches are particularly common. A recent report entitled *Trends in Cybersecurity Breach Disclosures* compiled by Audit Analytics reviewed 639 cybersecurity breaches at public companies since 2011. The report found that between 2011 and 2019, malware was the most commonly used method to carry out a cyberattack, with 34% of breaches reviewed being malware-based breaches.[15] The report identified that in 2018 and 2019, names and credit card information were the most highly-sought types of information in data breaches.[16]

154. During the period of the Data Breach, Visa specifically warned gas station operators about an increase in hackers targeting internal payment processing systems at fuel dispensers. The warning specified that hackers have been targeting internal processing systems, not just external card-swipe terminals attached to fuel dispensers.

155. Specifically, Visa distributed a "Security Alert" dated November 2019 stating the following, in relevant part:

> In August and September 2019, Visa Payment Fraud Disruption (PFD) investigated two separate breaches at North American fuel dispenser merchants. The attacks involved the use of point-of-sale (POS) malware to harvest payment card data from fuel dispenser merchant POS systems. It is important to note that **this attack vector differs significantly from skimming at fuel pumps, as the targeting of POS systems requires the threat actors to access the merchant's internal network**. In one of the two cases investigated by PFD, the threat actors successfully compromised the merchant's network through a phishing email that contained a malicious attachment. Once the malware was deployed on the merchant's network, it scraped Track 1 and Track 2 payment card data from the random access memory (RAM) of the targeted POS system. The threat actors were able to obtain this payment card data due to the lack of secure acceptance technology, (e.g. EMV®

[15] Mark Wilczek, *Average Cost of a Data Breach: $116M*, Commenting on Vulnerabilities/ Threats (June 24, 2020, 2:00 PM), https://www.darkreading.com/vulnerabilities---threats/average-cost-of-a-data-breach-$116m/a/d-id/1338121.
[16] *Id*.

> Chip, Point-to-Point Encryption, Tokenization, etc.) and non-compliance with PCI DSS.
>
> **The targeting of fuel dispenser merchants is the result of the slower migration to chip technology on many terminals, which makes these merchants an attractive target for criminal threat actors attempting to compromise POS systems for magnetic stripe payment card data**.
>
> * * *
>
> The recent attacks are attributed to two sophisticated criminal groups with a history of large-scale, successful compromises against merchants in various industries. The groups gain access to the targeted merchant's network, move laterally within the network using malware toolsets, and ultimately target the merchant's POS environment to scrape payment card data. The groups also have close ties with the cybercrime underground and are able to easily monetize the accounts obtained in these attacks by selling the accounts to the top tier cybercrime underground carding shops.
>
> Fuel dispenser merchants should take note of this activity as the group's operations are significantly more advanced than fuel dispenser skimming, and these attacks have the potential to compromise a high volume of payment accounts. The deployment of devices that support chip will significantly lower the likelihood of these attacks.[17]

156. In sum, the Visa warning plainly specified that hackers were placing "malware" onto card processing systems. Notably, Wawa has acknowledged that the Data Breach involved malware.[18] Thus, the risk that Visa warned gas station operators about was the exact risk that led to the Wawa Data Breach.

157. The Visa warning also specified that hackers were attacking gas stations that had not yet upgraded to chip technology at fuel dispensers. Notably, despite this warning, Wawa had not yet fully upgraded to chip technology at the time of the Data Breach.[19]

---

[17] Visa Security Alert (November 2019), *available at* https://usa.visa.com/dam/VCOM/global/support-legal/documents/visa-security-alert-attacks-targeting-fuel-dispenser-merchant-pos.pdf (last visited Jan. 9, 2020) (emphasis added).

[18] *See Wawa Notifies Customers of Data Security Incident (12/19/2019) Press Release,* Wawa Data Security Incident (Dec. 19. 2019), https://www.wawa.com/alerts/data-security.

[19] Christian Hetrick, *Before Wawa Found Data Breach Exposing Customers' Credit and Debit*

158. One data security expert noted that the Wawa Data Breach may have resulted from an employee clicking on a phishing link, which was the precise risk flagged by the Visa alert:

> Michael Levy, former chief of computer crimes at the U.S. Attorney's Office for the Eastern District of Pennsylvania, wrote in an email[:] … "[I]f you can get an employee inside the company to click on a link, and that link causes the employee's computer to download malware, you have tunneled under the moat and [fire]wall. It was my guess that the perpetrators accomplished the Wawa breach in a similar fashion."[20]

159. Robert Siciliano, a cybersecurity expert with ETF Managers Group, similarly stated that the hack could have occurred as the result of a single Wawa employee clicking on a nefarious link or email attachment, and that from there, hackers might have been able to forge a path to Wawa's payment servers.[21]

160. The Visa warning highlighted specific risk factors that were present within Wawa's payment card and computer systems and warned of the precise type of hacking that ultimately took place at Wawa. The Visa warning placed Wawa on further notice of an unusually high risk of a data breach. Wawa failed to improve its Card Information security and system monitoring procedures despite these known critical risks.

161. Furthermore, Wawa's data security obligations and promises were particularly important given the many high-profile payment card data breaches that have been reported in recent years, which were widely known to the public and to any entity, like Wawa, that conducts a substantial amount of business via payment cards. In recent years, massive payment card data

---

Cards, Visa Warned It Could Happen, THE PHILADELPHIA INQUIRER (Jan. 2, 2020), https://www.inquirer.com/business/wawa-visa-hacks-identity-theft-suits-20200102.html. ("Wawa said this week that it is implementing chip technology at gas pumps and expects all pumps to be upgraded in 2020.").

[20] *Id.*

[21] Stephen Yin, *The Wawa data breach: What happens now?*, WHYY (Dec. 27, 2019), https://whyy.org/articles/the-wawa-data-breach-what-happens-now/#:~:text=The%20breach%20itself,PIN%20numbers%20or%20security%20codes.

breaches have impacted large retailers and restaurants, including Arby's, Chipotle, Dairy Queen, Forever 21, GameStop, Harbor Freight Tools, Home Depot, Hy-Vee, Kmart, Lord & Taylor, Michael's Stores, Neiman Marcus, Noodles & Co., P.F. Chang's, Saks Fifth Avenue, Sally Beauty Supply, Schnuck Markets, SuperValu, Target, T.J. Maxx, Wendy's, and many others. Large breaches have impacted not just retailers and restaurants, but also large companies responsible for housing important and sensitive consumer financial and medical data. The high-profile breaches that impacted Marriott, Equifax, Yahoo, Premera, and Anthem serve as additional examples of the consequences of inadequate data security, and these breaches put Wawa on further notice of the need to have robust data security protections in place at its convenience store and fuel dispenser locations.

162. In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have "engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data," including recent cases against Uber Technologies, Venmo, and VTech Electronics.[22] The FTC has publicized these and other enforcement actions so that companies entrusted with sensitive financial information are aware of their duty and can improve their practices for safeguarding customer information.[23]

C. Wawa's Privacy Policy

163. Wawa's Privacy Policy states that data security is important to Wawa and that Wawa is committed to safeguarding consumer data:

> Protecting your privacy is important to Wawa. This Wawa Privacy Policy ("Policy") describes how Wawa and its subsidiaries and affiliated companies

[22] Fed. Trade Comm'n, Privacy & Data Security (2018), at p.5, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf.
[23] Fed. Trade Comm'n, *Start With Security: A Guide For Business, Lessons Learned From FTC Cases* (2015), at p. 1, https://www.bulkorder.ftc.gov/system/files/publications/pdf0205-startwithsecurity.pdf.

> collect, use, disclose and safeguard the personal information … collected when you visit our stores or otherwise communicate or interact with Wawa.
>
> * * *
>
> We may collect any information, such as your first and last name, credit card number, email address, postal address, and telephone number that you provide when you interact with Wawa. Some examples are when you: Make an online or in-store purchase ….
>
> * * *
>
> Data Security
>
> **Wawa is fully committed to data security**.[24]

164. Wawa further claims to "use security techniques on" its websites, "and through or in connection with our mobile apps or other software- and Internet-enabled programs and services sponsored by Wawa (the 'Sites')" to "help protect against the loss, misuse or alteration of information collected from [its customers] at the Sites." As Wawa puts it, when customers "access [their] account information or transmit personally identifiable data to the Sites, that information is stored on servers that the Sites have attempted to secure from unauthorized access or intrusion. 'Secure Socket Layer' software encrypts personal information [customers] transmit to the Sites."[25]

165. However, Secure Socket Layer ("SSL") encryption protects information only in the course of its transmission, and not upon its storage on Wawa systems. Moreover, SSL encryption "is not sufficiently secure."[26] Wawa has disclosed no further details about its efforts to secure its customers' data prior to the Data Breach.

166. Plaintiffs and class members provided their Card Information to Wawa with the reasonable expectation and mutual understanding that Wawa would comply with its obligations to

---

[24] Wawa Official Privacy Policy (last updated June 25, 2020), https://www.wawa.com/privacy (emphasis added).
[25] *Id.*
[26] *See* Internet Engineering Task Force, *Deprecating Secure Sockets Layer Version 3.0*, https://tools.ietf.org/pdf/rfc7568.pdf (last visited June 18, 2020).

keep the Card Information confidential, and would secure it from unauthorized access by intentional wrongdoers. Yet Wawa failed to do so, in contravention of its own privacy policy.

D. Wawa's Data Security Failures

167. According to Osano, a company building the first platform for data privacy transparency, there exists a "predictive relationship between responsible privacy practices and security outcomes" and companies with "inadequate data privacy practices are 80 percent more likely to suffer a data breach than those with the highest-ranked practices."[27] The occurrence of the Data Breach establishes that Wawa breached its duties and obligations by failing to, among other things, do the following:

a. Adequately safeguard consumers' Card Information;

b. Maintain an adequate data security environment to reduce the risk of a data breach;

c. Maintain periodic audits of its internal security systems, which would permit it to discovery any irregularities within a reasonable period of time;

d. Properly monitor its data security systems for existing intrusions and weaknesses throughout the nine-month period of the Data Breach;

e. Perform penetration tests to determine the strength of its payment card processing systems;

f. Properly train its information technology staff on matters relevant to Card Information security; and

g. Retain outside vendors to periodically test its payment card processing systems.

168. With respect to Wawa's monitoring procedures, industry experts have affirmed that the lengthy period of the Data Breach is indicative of Wawa's faulty monitoring systems:

> "What is most shocking to me, and should be most appalling to everybody, is how long this went undetected. How did Wawa just find this recently?" said Ron

[27] *See Organizations with poor privacy practices 80% more likely to suffer data breach*, HELP NET SECURITY (July 23, 2020), https://www.helpnetsecurity.com/2020/07/23/poor-privacy-practices/.

> Schlecht, managing partner at Bala Cynwyd-based BTB Security. "They were obviously not monitoring at an appropriate level commensurate with their business volume and were unable to detect this anomalous activity."[28]

169. As alleged in greater detail below, these shortfalls in data privacy measures also establish that Wawa violated the Payment Card Industry Data Security Standards ("PCI DSS"), as well as Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Wawa also failed to adhere to recommendations issued by the National Institute of Standards and Technology ("NIST").

170. Wawa had systemic failures in its overall network environment, not just within its cardholder data environment. The systemic failures are apparent because, among other things, the malware was able to impact virtually all Wawa locations, and ran without detection for nine months. The failures violated formal industry standards as well as common industry practices.

1. Wawa Violated the Payment Card Industry Data Security Standards

171. There is an extensive network of financial institutions, card-issuing banks, and card-processing companies involved in credit and debit card transactions. Card networks have issued detailed rules and standards governing the basic protective measures that merchants like Wawa must take to ensure that payment card information is properly safeguarded.

172. Furthermore, the payment card networks (primarily MasterCard, Visa, American Express, and Discover) have issued card operating rules that are binding on merchants, including Wawa, and require merchants to protect Card Information. In particular, the Payment Card Industry Security Standards Council promulgates minimum standards that apply to all

[28] Christian Hetrick, *Before Wawa Found Data Breach Exposing Customers' Credit and Debit Cards, Visa Warned It Could Happen*, THE PHILADELPHIA INQUIRER (Jan. 2, 2020), https://www.inquirer.com/business/wawa-visa-hacks-identity-theft-suits-20200102.html.

organizations that store, process, or transmit payment card data, known as PCI DSS. PCI DSS is the universal industry standard governing the security of credit and debit card data.

173. PCI DSS establishes detailed and comprehensive requirements for satisfying each of the following twelve "high-level" mandates:[29]

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7.** Restrict access to cardholder data by business need to know **8.** Identify and authenticate access to system components **9.** Restrict physical access to cardholder data
Regularly Monitor and Test Networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes
Maintain an Information Security Policy	**12.** Maintain a policy that addresses information security for all personnel

174. PCI DSS sets the *minimum* level of what must be done to protect the cardholder data environment ("CDE"). While PCI DSS compliance is an important first step in securing cardholder data such as the Card Information compromised in the Data Breach, it is not sufficient on its own to protect against compromises that may in turn breach the CDE, nor does it provide a safe harbor against civil liability for a data breach.

175. As noted in bullet 5 of the chart, PCI DSS required Wawa to "protect all systems against malware." Wawa patently failed to do so given the admission in its Data Breach

[29] *Payment Card Industry (PCI) Data Security Standard*, PCI SECURITY STANDARDS COUNCIL (May 2018), at p. 5, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1577046042482.

notification that the Data Breach involved hacker(s) placing "malware" on Wawa's payment processing servers.

176. PCI DSS at bullet 10 also required Wawa to "[t]rack and monitor all access to network resources and cardholder data." Wawa failed to do so, having admitted that the hacker(s) had access to its system for nine months. The nine-month delay in detecting the breach illustrates that Wawa had materially deficient tracking and monitoring systems in place.

177. Wawa violated numerous other provisions of PCI DSS, including subsections underlying the high-level mandates in the chart above. Those deficiencies will be revealed during discovery.

178. Industry experts acknowledge that a data breach is indicative of data security failures. For example, research and advisory firm Aite Group has stated: "'**If your data was stolen through a data breach that means you were somewhere out of compliance' with payment industry data security standards.**"[30]

179. Wawa was an active participant in the payment card networks as it collected and transmitted millions of sets of payment card data per day. At all relevant times, Wawa knew of its PCI DSS obligations to protect cardholder data such as the Card Information compromised in the Data Breach.

2. Wawa Violated the FTC Act

180. The Federal Trade Commission has held that the failure to employ reasonable measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act (codified by 15 U.S.C. §45).

[30] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017, 2:29 PM), https://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY (emphasis added).

181. Beginning in 2007, the FTC released a set of industry standards related to data security and the data security practices of businesses, called "Protecting Personal Information: A Guide for Businesses" (the "FTC Guide").[31] In 2011, this guidance was updated to include fundamental data security principles for businesses. In addition to the necessity to protect consumer data, the guide established that:

- Businesses should dispose of personal identifiable information that is no longer needed;
- Businesses should encrypt personal identifiable information and protected cardholder data stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;
- Businesses should thoroughly understand the types of vulnerabilities on their network (of which malware on a point-of-sale system is one) and how to address said vulnerabilities;
- Businesses should implement protocols necessary to correct security breaches;
- Businesses should install intrusion detection systems to expose security breaches at the moment they occur;
- Businesses should install monitoring mechanisms to watch for massive troves of data being transmitted from their systems; and
- Businesses should have an emergency plan prepared in response to a breach.

182. Wawa failed to adequately address the foregoing requirements in the FTC Guide.

183. In 2015, the FTC supplemented the FTC Guide once more with a publication called "Start with Security" (the "Supplemented FTC Guide").[32] This supplement added further requirements for businesses that maintain customer data on their networks:

---

[31] *See FTC Unveils Practice Suggestions for Businesses on Safeguarding Personal Information*, FEDERAL TRADE COMM'N (Mar. 8, 2007), https://www.ftc.gov/news-events/press-releases/2007/03/ftc-unveils-practical-suggestions-businesses-safeguarding; *see also* Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business, Federal Trade Commission* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (updated FTC Guide).

[32] Fed. Trade Comm'n, *Start with Security: A Guide for Business* (June 2015), https://www.ftc.gov

- Businesses should not keep personal identifiable information and protected cardholder data stored on their networks for any period longer than what is needed for authorization;
- Businesses should use industry-tested methods for data security; and
- Businesses should be continuously monitoring for suspicious activity on their network.

184. Again, Wawa failed to adequately address these requirements enumerated in the Supplemented FTC Guide.

185. The FTC Guide is clear that businesses should, among other things: (1) protect the personal customer information they acquire; (2) properly dispose of personal information that is no longer needed; (3) encrypt information stored on computer networks; (4) understand their network's vulnerabilities; and (5) implement policies for installing vendor-approved patches to correct security vulnerabilities. The FTC guidance also recommends that businesses: (1) use an intrusion detection system to expose a breach as soon as it occurs; (2) monitor all incoming traffic for activity indicating that someone may be trying to penetrate the system; and (3) watch for large amounts of data being transmitted from the system.[33] Wawa did not do these things, and as a result exposed millions of consumers to harm.

186. Furthermore, the FTC has issued orders against businesses for failing to employ reasonable measures to safeguard customer data. The orders provide further public guidance to businesses concerning their data security obligations.

/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[33] *See, e.g.*, *id.*; Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

187. Wawa knew or should have known about its obligation to comply with the FTC Act, the FTC Guide, the Supplemented FTC Guide, and many other FTC pronouncements regarding data security.

188. Wawa's misconduct violated the FTC Act and the FTC's data security pronouncements, led to the Data Breach, and resulted directly and proximately in harm to Plaintiffs and class members.

3. Wawa Disregarded Guidance Established by the National Institute of Standards and Technology

189. The National Institute of Standards and Technology provides basic network security guidance that enumerates steps to take to avoid cybersecurity vulnerabilities.[34] Although use of NIST guidance is voluntary, the guidelines provide valuable insights and best practices to protect network systems and data.

190. NIST guidance includes recommendations for risk assessments, risk management strategies, system access controls, training, data security, network monitoring, breach detection, and mitigation of existing anomalies.[35]

191. Wawa's failure to protect massive amounts of Card Information throughout the nine-month breach period belies any assertion that Wawa employed proper data security protocols or adhered to the spirit of the NIST guidance.

[34] *Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (April 16, 2018), Appendix A, Table 2, *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[35] *Id*. at Table 2 pg. 26-43.

E. As Many as 30 Million Payment Cards May Have Been Impacted by the Data Breach; Stolen Data Has Been Offered for Sale on the "Dark Web"; and Misuse of the Stolen Data Is Ongoing

192. Widespread misuse of the stolen Card Information has already begun and, as alleged herein, Plaintiffs have already suffered fraudulent charges on their payment cards.

193. Visa and MasterCard have issued Compromised Account Management System ("CAMS") alerts to card-issuing banks and credit unions to highlight the risk of fraud on the issuers' payment cards used at Wawa during the Data Breach period.

194. In reaction to the risk of fraudulent transactions, some card issuers have sent replacement cards to thousands of customers who used their payment cards at Wawa during the period of the Data Breach.[36] Given the significant cost of issuing replacement cards, banks generally do not preemptively issue replacement cards unless the risk of fraud is high in light of the facts of the particular breach and the presence of fraudulent activity on at least some of the cards stolen in the breach.

195. On January 28, 2020, a New-York based cybersecurity and fraud intelligence company, Gemini Advisory, stated that the Wawa Data Breach involved approximately 30 million payment cards, and that some of the stolen card information had been offered for sale on one of the most notorious websites for buying and selling stolen credit card information, called "Joker's Stash":

> The Joker's Stash marketplace, one of the largest and most notorious dark web marketplaces for buying stolen payment card data, has advertised its next major breach . . . . The latest advertisement claimed that the cards would go live on January 27, 2020 at 11:00 PM EST. The full collection would include **30 million US records** across more than 40 states . . . .

[36] Christian Hetrick, *After Wawa Breach, Banks Reissue Thousands of Debit, Credit Cards to Customers*, THE PHILADELPHIA INQUIRER (last updated Jan. 3, 2020), https://www.inquirer.com/news/wawa-citibank-citizens-bank-credit-debit-breach-hack-20200103.html.

> Joker's Stash began uploading records as advertised on January 27. The breach was titled "BIGBADABOOM-III" and appeared in four different bases. . . .
>
> **Gemini has determined that the point of compromise for BIGBADABOOM-III is Wawa**, an East Coast-based convenience store and gas station. . . . .
>
> **Since the breach may have affected over 850 stores and potentially exposed 30 million sets of payment records, it ranks among the largest payment card breaches of 2019, and of all time**. It is comparable to Home Depot's 2014 breach exposing 50 million customers' data or to Target's 2013 breach exposing 40 million sets of payment card data. . . .
>
> . . . .
>
> **The median price of US-issued records from this breach is currently $17** . . . .[37]

196. According to the popular cybersecurity website Krebs on Security, on January 27, 2020, Joker's Stash "began selling card data from 'a new huge nationwide breach' that purportedly includes more than 30 million card accounts issued by thousands of financial institutions across more than 40 U.S. states."[38] Krebs further confirmed that the payment card data for sale on Joker's Stash was stolen from Wawa, stating: **"Two sources that work closely with financial institutions nationwide tell KrebsOnSecurity the new batch of cards that went on sale Monday evening – dubbed 'BIGBADABOOM-III' by Joker's Stash – map squarely back to cardholder purchases at Wawa**."[39]

---

[37] Stas Alforov and Christopher Thomas, *Breaches Wawa payment Records Reach Dark Web*, Posted on Gemini Advisory Blog (Jan. 28, 2020), https://geminiadvisory.io/breached-wawa-payment-card-records-reach-dark-web/ (emphasis added).

[38] *Wawa Breach May Have Compromised More Than 30 Million Payment Cards*, KREBSONSECURITY (Jan. 28, 2020), https://krebsonsecurity.com/2020/01/wawa-breach-may-have-compromised-more-than-30-million-payment-cards/.

[39] *Id.* (emphasis added).

197. On January 28, 2020, *The Philadelphia Inquirer* reported that "Wawa said . . . that it was aware of reports that criminals tried to sell information that could have been taken during its data breach …. [and that] it has alerted its payment card processor, payment card brands, and card issuers to 'heighten fraud monitoring activities.'"[40] A later article from the *Legal Intelligencer* dated February 20, 2020 also noted that "[r]eports indicate customer data from the [Wawa] breach is now for sale on the dark web and the total number of compromised payment card accounts may reach 30 million."[41]

198. Another data security expert, Flare Systems, stated that **the stolen Wawa data likely began being sold in stages throughout 2019 prior to being offered for sale in bulk on Joker's Stash**. Flare Systems noted that the data was likely sold "over the course of 2019 in small batches, by organized gangs to a limited circle of malicious actors." Thereafter, "when news broke about Wawa's hack on December 19, 2019, the sale of Wawa credit cards probably slowed or stopped, only to be resumed on Joker's Stash the following month at a discounted price given their now tainted nature."[42]

199. Indeed, fraudulent charges on Plaintiffs' payment cards began occurring prior to Wawa's announcement of the Data Breach and before the Wawa payment card dump became available on Joker's Stash.

---

[40] *See* Christian Hetrick, *Millions of Cards Exposed in Wawa Breach are Up For Sale Online, Cybersecurity Experts Say*, THE PHILADELPHIA INQUIRER (last updated Jan. 28, 2020), https://www.inquirer.com/consumer/technology/wawa-data-breach-cards-sale-jokers-stash-krebs-20200128.html.

[41] *See* Patrick McKnight, *Wawa Data Breach Could Impact 30 Million Payment Cards*, THE LEGAL INTELLIGENCER (Feb. 20, 2020, 1:49 PM), https://www.law.com/thelegalintelligencer/2020/02/20/wawa-data-breach-could-impact-30-million-payment-cards/.

[42] *See* David Hétu, *The Truth Behind Joker's Stash / Wawa Announcement*, Posted to Flare Systems Blog (Feb. 7, 2020), https://flare.systems/blog/the-truth-behind-jokers-stash-wawa-announcement/.

200. Wawa issued a statement that "[d]ebit card PIN numbers, credit card CVV2 numbers (the three or four-digit security code printed on the card), [and] other PIN numbers ... were not affected by [the Data Breach]."[43] However, the popular tech news website ZDNet.com obtained a sample of the payment card data for sale on Joker's Stash, and CVV2 numbers were in fact included.[44] ZDNet stated that "according to a sample of the Wawa card dump obtained by ZDNet, the card dump did include CVV2 numbers, despite Wawa's claims."[45]

201. Wawa has implicitly acknowledged that payment card fraud has taken place as a result of the Data Breach. When Wawa first announced the Data Breach, it stated that "[a]t this time, Wawa is not aware of any unauthorized use of any payment card information as a result of this incident." Wawa has since deleted that sentence from the Data Breach announcement page on its website.[46]

202. According to a *Forbes* article, Joker's Stash prides itself on selling payment card data stolen from large data breaches.[47] Joker's Stash has uploaded records from several major breaches in the past, including those that impacted Lord & Taylor and Saks Fifth Avenue.[48] A number of other recent high-profile nationwide payment card breaches have been linked to large numbers of cards for sale at Joker's Stash, including breaches at Bebe Stores, Buca di Beppo, Hy-

---

[43] *See supra*, note 4.
[44] *See* Catalin Cimpanu, *Wawa's Massive Card Breach: 30 Million Customers' Details for sale Online*, ZERO DAY NET (Jan. 28, 2020), https://www.zdnet.com/article/wawa-card-breach-may-rank-as-one-of-the-biggest-of-all-times/.
[45] *Id*.
[46] https://www.wawa.com/alerts/data-security.
[47] *See* Davey Winder, *Joker's Stash Asks $130 Million for Stolen Credit Card Database*, FORBES (Nov. 8, 2019, 10:43 AM), https://www.forbes.com/sites/daveywinder/2019/11/08/jokers-stash-asks-130-million-for-stolen-credit-card-database/#336455b510e9.
[48] Stas Alforov and Christopher Thomas, *Breaches Wawa payment Records Reach Dark Web*, Posted on Gemini Advisory Blog (Jan. 28, 2020), https://geminiadvisory.io/breached-wawa-payment-card-records-reach-dark-web/.

Vee, Hilton Hotels, Krystal, McAlister's Deli, Moe's, Schlotzsky's, and Sonic.[49] Joker's Stash is said to pose an evolving and enduring threat to consumers and retailers, with an infrastructure consisting of over 50 servers and an extensive online presence of more than 500 associated domains. These domains are typically rolled out in advance of surges in available data in order to better support people buying bulk information obtained through unlawful data breaches such as this one.[50] Researchers at Recorded Future security intelligence say that these domains "act as portals for Joker's Stash's biggest clients to have dedicated servers to purchase, store, and retrieve cards of interest."[51]

203. In 2015, Joker's Stash moved to using Blockchain DNS, which allows website visitors to avoid attempted government censorship or surveillance.[52]

F. Damages to Class Members

204. Wawa's data security failures are particularly alarming given that the breach lasted nine months and impacted all or nearly all of Wawa's approximately 900 locations. Each Plaintiff and the class members have been damaged by the compromise of their Card Information in the Data Breach.

205. As alleged in detail above, class members have already been damaged to the extent that their Card Information is among the 30 million records believed to be extracted by way of the Wawa Data Breach and offered for sale on the "dark web."

---

[49] *See supra*, note 38.
[50] Tara Seals, *Joker's Stash Drops Largest-Ever Credit Card Cache on Dark Web*, THREAT POST (Oct. 29, 2019), https://threatpost.com/jokers-stash-largest-ever-credit-card-drop/149649/.
[51] Mathew Schwartz, *Joker's Stash Lists 1.3 Million Stolen Indian Payment Cards*, BANK INFO SECURITY (Oct. 29, 2019), https://www.bankinfosecurity.com/jokers-stash-lists-13-million-indian-payment-cards-a-13302.
[52] *What Fraud Teams Need to Know About Joker's Stash*, Payment Industry Intelligence: Payment Cards & Mobile (Nov. 13, 2019), https://www.paymentscardsandmobile.com/what-fraud-teams-need-to-know-about-jokers-stash/.

206. Class members also face a substantial and imminent risk of fraudulent charges on their payment cards. Criminals carried out the Data Breach and stole the Card Information with the intent to use it for fraudulent purposes themselves and/or to sell it, which has already been confirmed to have occurred on Joker's Stash and the dark web.

207. Moreover, as alleged in greater detail above, Plaintiffs and class members have already experienced fraudulent credit and debit card transactions, and other class members are at a significantly enhanced risk of experiencing payment card fraud going forward.

208. Also, certain Plaintiffs and class members have already incurred or will incur out-of-pocket costs for protective measures (*e.g.*, credit monitoring fees, credit report fees, and credit freeze fees), fees for replacement cards, overdraft fees, late payment fees owed to vendors, and similar costs related to the Data Breach.

209. Class members also suffered a "loss of value" of their credit and debit card information when it was stolen by the hacker(s) in the Data Breach. A robust market exists for stolen card information, which is sold on the dark web at specific identifiable prices, such as the Data Breach Card Information already for sale on Joker's Stash.

210. Class members also suffered "benefit of the bargain" damages. Class members overpaid for goods that should have been—but were not—accompanied by adequate data security. Part of the price class members paid to Wawa was intended to be used to fund adequate data security. Thus, by way of the Data Breach, class members did not get what they paid for. Had class members known the truth about Wawa's deficient data security practices, they would not have used their payment cards at Wawa, or they would have been unwilling to pay full price for their purchases.

211. Class members have spent and will continue to spend substantial amounts of time monitoring their payment card accounts for fraud, disputing fraudulent transactions, and reviewing their financial affairs more closely than they otherwise would have done but for the Data Breach. Class members will also spend time obtaining replacement cards and resetting automatic payment links to their new cards, among other things. These efforts are burdensome and time-consuming and would not be necessary but for Wawa's data security shortfalls.

212. Class members who experience actual fraud are also harmed by the inability to use their credit or debit cards when their accounts are suspended or otherwise rendered unusable due to the fraudulent charges. Class members are also harmed by the loss of use of and access to their account funds, or being limited in the amount of money they are permitted to obtain from their accounts, while fraudulent charges are investigated but not yet reversed. The lag time between when fraudulent charges are incurred and when they are reversed may take several days or weeks.

213. Class members who experienced fraudulent card transactions may also be harmed by having to forfeit rewards points or airline miles they earned on payment cards that were cancelled, or by not being able to earn points or miles on transactions they could not make on their rewards cards while awaiting replacement cards.

214. Class members who experienced fraudulent card transactions and lost access to the stolen funds for days or weeks may also be harmed due to missed payments on bills and loans, late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations from unpaid credit card bills.

215. The stolen Card Information is a valuable commodity to identity thieves. William P. Barr, the United States Attorney General, has recently stated that consumers' sensitive personal

information commonly stolen in data breaches "has economic value."[53] The purpose of stealing large caches of Card Information is to use it to defraud consumers or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit payment card fraud. Indeed, cyber criminals routinely post stolen payment card information on anonymous websites, making the information widely available to a criminal underworld. There is an active and robust market for this information.

216. Indeed, the fact that the payment cards compromised in the data breach were reportedly available for sale for $17 per card on the dark web demonstrates that this information was of considerable value to fraudsters. The purpose of stealing large caches of Card Information is to use it to defraud consumers or to place it for illegal sale and to profit from other criminals who buy the data and use it to commit payment card fraud.

217. Cyber criminals routinely post stolen payment card information on untraceable dark web commerce sites—such as the large batches of card information offered for sale on Joker's Stash—making the information widely available to a criminal underworld for an open, indefinite period of time. There is an active and robust market for this information.

i. The Stolen Data is at Risk of Misuse for Years

218. The risk of fraud following a data breach persists for years. Identity thieves sometimes hold stolen data for months or years before using it, to avoid detection. Also, the sale of stolen information on the dark web may take months or more to reach end-users, in part because the data is often sold in small batches as opposed to in bulk to a single buyer.

[53] *See* Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax, U.S. DEP'T OF JUSTICE, (Feb. 10, 2020), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military (last visited July 24, 2020).

219. According to a GAO Report, the threat of future identity theft lingers for a substantial period of time after a data breach given the time lag between when information is stolen and when it is used:

> [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.[54]

220. Thus, class members face an ongoing risk and must vigilantly monitor their financial accounts for months or years to come.

ii. Class Members Face a Risk of Identity Theft Beyond Just Credit and Debit Card Fraud

221. Identity thieves can combine data stolen in the Data Breach with other information about class members gathered from other data breaches, underground sources, public sources, or even class members' social media accounts to commit a wide array of fraud. Thieves can also use the combined data to send highly targeted phishing emails to class members to obtain more sensitive information. Thieves can then use the combined data to commit potential crimes including—among other things—opening new financial accounts in class members' names, taking out loans in class members' names, using class members' information to obtain government benefits, filing fraudulent tax returns using class members' information, obtaining driver's licenses in class members' names but with another person's photograph, and giving false information to police during an arrest.[55]

---

[54] *See Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown*, United States Government Accountability Office (June 2007), https://www.gao.gov/assets/270/262899.pdf.

[55] *See* Fed. Trade Comm'n, *Warning Signs of Identity Theft*, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited June 19, 2020).

222. Wawa has acknowledged that class members face a risk of various types of identity theft stemming from the Data Breach, even beyond payment card fraud. Wawa recommended that affected customers undertake the following tasks in response to the Data Breach: (i) "Review Your Payment Card Account Statements" and "notify the relevant payment card company" if "there is an unauthorized charge on your payment card"; (ii) "Order a Credit Report" and "review the entire report carefully" to "look for any inaccuracies and/or accounts you don't recognize, and notify the credit bureaus as soon as possible in the event there are any"; (iii) place a "fraud alert" on your credit file to "protect you against the possibility of an identity thief opening new credit accounts in your name"; and (iv) place a "security freeze" on your credit file to prevent creditors from accessing the credit file without the consumer's consent.[56] Thus, Wawa acknowledged that class members face a risk of identity theft beyond just fraudulent credit and debit card transactions. Wawa would not have made these recommendations if there were no risk of identity theft from the Data Breach.

223. To protect against these various types of fraud, Wawa has offered only one year of free credit monitoring and identity theft insurance to customers whose card information was stolen in the Data Breach. This limited offering of protection is insufficient. Credit monitoring coverage and identity theft insurance are needed for much longer than just one year. Furthermore, the fact that Wawa offered credit monitoring illustrates that consumers face a risk of identity theft beyond just payment card fraud.

[56] *See supra*, note 4.

V. CLASS ACTION ALLEGATIONS

224. Plaintiffs bring this case as a class action pursuant to Fed. R. Civ. P. 23(a), (b)(2) and (b)(3) on behalf of a Nationwide Class or, in the alternative, on behalf of the State Classes (collectively, the "Classes") as defined below:

> Nationwide Class: All persons in the United States who used a credit or debit card at a Wawa location impacted by the Data Breach that was announced by Wawa on December 19, 2019, at any time during the period of the Data Breach.
>
> Delaware Class: All persons who used a credit or debit card at a Delaware Wawa location impacted by the Data Breach that was announced by Wawa on December 19, 2019, at any time during the period of the Data Breach.
>
> Florida Class: All persons who used a credit or debit card at a Florida Wawa location impacted by the Data Breach that was announced by Wawa on December 19, 2019, at any time during the period of the Data Breach.
>
> Maryland Class: All persons who used a credit or debit card at a Maryland Wawa location impacted by the Data Breach that was announced by Wawa on December 19, 2019, at any time during the period of the Data Breach.
>
> New Jersey Class: All persons who used a credit or debit card at a New Jersey Wawa location impacted by the Data Breach that was announced by Wawa on December 19, 2019, at any time during the period of the Data Breach.
>
> Pennsylvania Class: All persons who used a credit or debit card at a Pennsylvania Wawa location impacted by the Data Breach that was announced by Wawa on December 19, 2019, at any time during the period of the Data Breach.
>
> Virginia Class: All persons who used a credit or debit card at a Virginia Wawa location impacted by the Data Breach that was announced by Wawa on December 19, 2019, at any time during the period of the Data Breach.
>
> District of Columbia Class: All persons who used a credit or debit card at a District of Columbia Wawa location impacted by the Data Breach that was announced by Wawa on December 19, 2019, at any time during the period of the Data Breach.

225. Excluded from Classes are Wawa's executive officers, and the judge to whom this case is assigned.

226. Numerosity. The Classes are each so numerous that joinder of all members is impracticable. On information and belief, each of the Classes consists of millions of individuals.

These estimates are based on the fact that the Data Breach affected most or all of Wawa's convenience store locations for a nine-month period, and reports that some 30 million cards have been stolen in the Data Breach.

227. Commonality. There are many questions of law and/or fact common to Plaintiffs and the Classes. Common questions include, but are not limited to, the following:

a. Whether Wawa's data security systems prior to and during the Data Breach complied with applicable data security laws, regulations, industry standards, and PCI DSS requirements;

b. Whether Wawa owed a duty to class members to safeguard their payment card information;

c. Whether was negligent or reckless in permitting the Data Breach to occur;

d. Whether Wawa had and breached implied contractual obligations to Plaintiffs and Class members;

e. Whether Wawa violated its own privacy policies and procedures;

f. Whether Wawa provided Plaintiffs and class members with adequate notification of the breach, and made available to them sufficient relief in response to it;

g. Whether Wawa breached its duty to class members to safeguard their payment card information;

h. Whether a computer hacker obtained class members' payment card information in the Data Breach;

i. Whether Wawa knew or should have known that its data security systems and monitoring processes were deficient;

j. Whether Plaintiffs and class members suffered legally cognizable damages as a result of the Data Breach; and

k. Whether Plaintiffs and class members are entitled to injunctive relief.

228. Typicality. Plaintiffs' claims are typical of the claims of all class members because Plaintiffs, like other class members, suffered a theft of their Card Information in the Data Breach.

229. Adequacy of Representation. Plaintiffs will fairly and adequately protect the interests of the Classes. Plaintiffs have retained competent and capable counsel with significant experience in complex class action litigation, including data breach class actions. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the Classes. Plaintiffs' counsel has the financial and personnel resources to do so. Neither Plaintiffs nor their counsel have interests that are contrary to, or that conflict with, those of the Classes.

230. Predominance. Wawa has engaged in a common course of conduct toward all class members. The common issues arising from Wawa's conduct predominate over any issues affecting just individual class members. All of the relevant common questions in this case are centered on Wawa's conduct, rather than that of any Plaintiff or class member. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

231. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would find that the cost of litigating their individual claim is prohibitively high, and they would have no effective remedy on an individual basis. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to class members, which would establish incompatible standards of conduct for Wawa. In contrast,

conducting this action on a class-wide basis presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of all class members.

232. Wawa has acted on grounds that apply generally to the Classes as a whole, so that injunctive relief is appropriate on a class-wide basis pursuant to Fed. R. Civ. P. 23(b)(2).

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of the Nationwide Class or, in the Alternative, the State Classes)

233. Plaintiffs re-allege and incorporate by reference all allegations in paragraphs 1 through 232 as if fully set forth herein.

234. This claim is pleaded on behalf of Plaintiffs and the Nationwide Class or, in the alternative, the Delaware, Florida, Maryland, New Jersey, Pennsylvania, Virginia, and District of Columbia Classes pursuant to the common law of those jurisdictions.

235. Wawa obtained credit and debit Card Information from Plaintiffs and members of the Class in connection with class members' purchases at Wawa's stores.

236. By collecting and maintaining Card Information, Wawa had a duty of care to use reasonable means to secure and safeguard the Card Information and to prevent disclosure of the information to unauthorized individuals. Wawa's duty included a responsibility to implement processes by which it could detect a data breach of the type and magnitude of the Data Breach in a timely manner.

237. Wawa also owed a duty of care to Plaintiffs and members of the Class to provide data security consistent with the various requirements and rules discussed above, including but not limited to PCI DSS, FTC guidance, and common law and statutory duties.

238. Wawa's duty of care arose as a result of, among other things, the special relationship that existed between Wawa and its customers. Wawa was in a position to ensure that

its systems were sufficient to protect against the foreseeable risk that a data breach could occur, which would result in substantial harm to consumers. Indeed, Wawa's announcement of the Data Breach acknowledged that Wawa was in a "special relationship" with its customers for purposes of protecting their Card Information.[57]

239. Wawa was subject to an "independent duty," untethered to any contract between Wawa and Plaintiffs or members of the Class.

240. Wawa breached its duties by failing to use reasonable measures to protect Card Information. Wawa breached its duties through acts and omissions that include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Card Information;

b. Failing to adequately monitor the security of Wawa's payment card processing network throughout the nine-month period of the Data Breach;

c. Allowing unauthorized access to the sensitive Card Information of Plaintiffs and Class members;

d. Failing to detect in a timely manner that the Card Information of Plaintiffs and Class members had been compromised; and

e. Failing to timely notify Plaintiffs and Class members about the Data Breach so that they could take appropriate steps to mitigate the risk of identity theft and other damages.

[57] *See An Open Letter from Wawa CEO Chris Gheysens to Our Customers* (Dec. 19. 2019), at https://www.wawa.com/alerts/data-security.

241. It was foreseeable to Wawa that its actions and omissions in failing to use reasonable measures to protect Card Information could result in injury to consumers, creating a foreseeable zone of risk to Plaintiffs and Class members.

242. Further, actual and attempted breaches of data security were reasonably foreseeable to Wawa given the known frequency of payment card data breaches: (i) in the retail industry in general, (ii) at fuel dispensers in particular, and (iii) at Wawa's operations specifically.

243. But for Wawa's failure to employ reasonable security measures as outlined above, the Card Information of Plaintiffs and Class members would not have been compromised, and the injuries detailed herein would not have occurred.

244. Plaintiffs and Class members have suffered, and continue to suffer, various types of damages as alleged above. The Card Information of Plaintiffs and Class members was targeted in the Data Breach, and their compromised information was highly sensitive, not easily replaceable, and can be used over a long period of time. Further, the confidential information of Plaintiffs and Class members has been accessed, offered for sale on the dark web, and/or misused. Plaintiffs and Class members have incurred damages as set forth above, including but not limited to: fraudulent transactions on their credit and/or debit cards; inability to use their credit and/or debit cards while those fraudulent transactions were being investigated and/or resolved and replacement cards were being issued; out of pocket costs related to credit monitoring fees, credit report fees, credit freeze fees, card replacement fees, bank fees, late fees, and other related costs; loss of value of their credit and debit card information; benefit of bargain damages; and lost time spent responding to the Data Breach.

245. Wawa's acts, omissions, and other wrongful conduct actually and proximately caused damages to Plaintiffs and Class members.

246. Additionally, the Delaware, Florida, Maryland, New Jersey, Pennsylvania, Virginia, and District of Columbia consumer protection acts[58] (the "State Consumer Protection Acts") and Section 5 of the FTC Act, 15 U.S.C. § 45, prohibit persons from engaging in unfair, abusive, or deceptive trade practices. The purpose of the State Consumer Protection Acts and the FTC Act are, at least in part, to protect the interests of consumers who entrust their confidential data to companies like Wawa. Various FTC publications, regulations, and orders also form the basis of Wawa's duties.

247. Wawa had a duty to employ reasonable security measures under the State Consumer Protection Acts and Section 5 of the FTC Act, as interpreted and enforced by the FTC, including using reasonable measures to protect confidential Card Information, which Wawa failed to do.

248. Wawa's duty to use reasonable care in protecting Card Information arose not only as a result of the statutes and regulations described above, but also because Wawa is bound by industry standards and PCI DSS to protect Card Information.

249. The State Consumer Protection Acts and Section 5 of the FTC Act apply to Wawa's acts and omissions alleged herein. Wawa's actions and inactions in failing to use reasonable measures to protect payment card data and in failing to comply with applicable industry standards violated the State Consumer Protection Acts and the FTC Act.

[58] *See* Delaware Consumer Fraud Act, 6 Del. Code §§ 2513, *et seq.*; Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.201, *et seq.* ("FDUTPA"); Maryland Consumer Protection Act, Md. Code Ann. Com. Law § 13-101, *et seq.*; New Jersey Consumer Fraud Act, N.J. Stat. Ann. §§ 56:8-1, *et seq.*; Pennsylvania Unfair Trade Practices And Consumer Protection Law, 73 Pa. Stat. §§ 201-1 to 201-9.2 ("UTPCPL"); Virginia Consumer Protection Act, Va. Code Ann. §§ 59.1-196, *et seq.*, and District Of Columbia Consumer Protection Procedures Act, D.C. Code §§ 28-3901, *et seq.* ("D.C. CPPA").

250. Wawa's acts and omissions, constituting violations of the State Consumer Protection Acts and Section 5 of the FTC Act, caused the type of harm those laws were intended to prevent, namely, damages and injury due to unlawful consumer practices.

251. Wawa's acts and omissions constituting violations of the State Consumer Protection Acts and Section 5 of the FTC Act are further evidence of Wawa's negligence, and actually and proximately caused the damages suffered by Plaintiffs and the Class members, as described herein.

252. Plaintiffs and Class members are entitled to compensatory, consequential, and other damages suffered as a result of the Data Breach.

253. Plaintiffs and Class members are also entitled to injunctive relief requiring Wawa to, *inter alia*: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide several years of free credit monitoring and identity theft insurance to all Class members.

254. The overall public interest of ensuring secure electronic payment platforms for all consumers is furthered by the remedies sought herein. These remedies will compensate Wawa customers injured by Wawa's breach of its duties to them and will ensure that consumers who made purchases at Wawa stores and fuel dispensers during the Data Breach period are protected from further breaches of the Card Information they used to make credit and debit card purchases.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of the Nationwide Class or, in the Alternative, the Delaware, Florida, New Jersey, Pennsylvania, Virginia, and District of Columbia Classes)

255. Plaintiffs re-allege and incorporate by reference all allegations in paragraphs 1 through 232 as if fully set forth herein.

256. This claim is pleaded on behalf of Plaintiffs and the Nationwide Class or, in the alternative, the Delaware, Florida, New Jersey, Pennsylvania, Virginia, and District of Columbia Classes pursuant to the common law of those jurisdictions.

257. Section 5 of the FTC Act prohibits, in relevant part, "unfair . . . practices in or affecting commerce." 15 U.S.C § 45(a). The purpose of the FTC Act is, at least in part, to protect the interests of consumers like Plaintiffs and Class members, who entrust their confidential data to companies like Wawa. As alleged in greater detail above, and incorporated herein by reference, various FTC publications, regulations, and orders also form the basis of Wawa's duties.

258. Plaintiffs and Class members are consumers within the class of persons Section 5 of the FTC Act and similar state statutes are intended to protect.

259. Wawa had a duty to employ reasonable security measures under Section 5 of the FTC Act, including, as interpreted and enforced by the FTC, using reasonable measures to protect confidential consumer payment card data, which Wawa failed to do.

260. Wawa's duty to use reasonable care in protecting the Card Information arose not only as a result of the statutes and regulations described above, but also because Wawa is bound by industry standards and PCI DSS to protect Card Information.

261. Section 5 of the FTC Act applies to Wawa's acts and omissions alleged herein. Wawa's actions in failing to use reasonable measures to protect payment card data and in failing to comply with applicable industry standards violated Section 5 of the FTC Act.

262. Wawa's acts and omissions, constituting violations of Section 5 of the FTC Act, were the cause in fact and proximate cause of the damages suffered by Plaintiffs and Class members, as described herein.

263. Moreover, Wawa engaged in unfair methods of competition, and unfair, deceptive, unconscionable, and unlawful acts or practices in the conduct of trade or commerce, in violation of the State Consumer Protection Acts as described *infra.*

264. The purpose of the State Consumer Protection Acts is, at least in part, to protect the interests of consumers like Plaintiffs and Class members, who entrust their confidential payment card data to companies like Wawa.

265. Wawa had a duty to employ reasonable security measures under those State Consumer Protection Acts, including using reasonable measures to protect confidential consumer data.

266. The State Consumer Protection Acts apply to Wawa's acts and omissions alleged herein. Wawa's actions in failing to use reasonable measures to protect payment card data and in failing to comply with applicable industry standards violated the State Consumer Protection Acts as discussed *infra*.

267. Wawa's acts and omissions caused the type of harm that the State Consumer Protection Acts were intended to prevent, namely, damages due to consumer deception, fraud, false pretense, false promise, misrepresentation, or the concealment, suppression, or omission of any material fact with intent that others rely upon the same in connection with the sale of merchandise.

268. Upon information and belief, Wawa also failed to satisfy the requirements of, and breached its duties under, the various State Data Breach Notification Laws of the jurisdictions in which Wawa operates, as described *infra*.[59]

[59] *See* 6 Del. Code Ann. § 12B-102(a) and (c); 6 Del. Code Ann. § 12B-101(2); Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2); N.J. Stat. Ann. § 56:8-163(a); District of Columbia Consumer Security Breach Notification Act, D.C. Code §§ 28-3851, *et seq*.; Virginia Personal

269. Wawa's unexcused wrongful acts and omissions, constituting violations of the State Consumer Protection Acts and State Data Breach Notification Laws, actually and proximately caused the harm suffered by Plaintiffs and Class members, as described herein.

270. Accordingly, Wawa's acts and omissions were negligent *per se*, and Plaintiffs and Class members are entitled to compensatory, consequential, and other damages.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class or, in the Alternative, the State Classes)

271. Plaintiffs re-allege and incorporate by reference all allegations in paragraphs 1 through 232 as if fully set forth herein.

272. This claim is pleaded on behalf of Plaintiffs and the Nationwide Class or, in the alternative, the Delaware, Florida, Maryland, New Jersey, Pennsylvania, Virginia, and District of Columbia Classes pursuant to the common law of those jurisdictions.

273. When Plaintiffs and Class members provided their Card Information to Wawa in exchange for Wawa's products, they entered into implied contracts with Wawa under which—and by mutual assent of the parties—Wawa agreed to take reasonable steps to protect the Card Information.

274. Wawa solicited and invited Plaintiffs and Class members to provide their Card Information as part of Wawa's regular business practices and as essential to the sales transaction process for card payment transactions. This conduct thus created implied contracts between Plaintiffs and Class members on one hand, and Wawa on the other hand. Plaintiffs and Class members accepted Wawa's offers by providing their Card Information to Wawa in connection with purchases at Wawa.

Information Breach Notification Act, Va. Code. Ann. §§ 18.2-186.6; *see also* Counts XI and XIII, *infra*.

275. When entering into the implied contracts, Plaintiffs and Class members reasonably believed and expected that Wawa's data security practices complied with relevant laws, regulations, and industry standards.

276. Wawa's implied promise to safeguard Card Information is evidenced by, *e.g.*: (i) the representations in Wawa's Privacy Policy set forth above; (ii) a duty to protect and safeguard Card Information that Wawa required Plaintiffs and Class members to provide as a condition of entering into credit and debit card transactions with Wawa; and (iii) Wawa's acceptance of Visa and MasterCard cards, which inherently implies that Wawa complies with Visa and Mastercard's data security rules because all merchants must comply with card network data security rules as a condition of accepting the cards.[60]

277. Plaintiffs and Class members paid money to Wawa to purchase items at Wawa's convenience stores and fuel dispensers. Plaintiffs and Class members reasonably believed and expected that Wawa would use part of those funds to obtain adequate data security. Wawa failed to do so.

278. Plaintiffs and Class members, on the one hand, and Wawa, on the other hand, mutually intended—as inferred from Wawa's Privacy Policy and its customers' continued use of its card payments system to make purchases from Wawa—that Wawa would adequately safeguard Card Information. Wawa failed to honor the parties' understanding of these contracts, causing injury to Plaintiffs and members of the Class.

---

[60] *See, e.g.*, Visa's "Card Acceptance Guidelines for Visa Merchants", 2017, at p. 65 ("PCI DSS compliance is required of all entities that store, process, or transmit Visa cardholder account and transaction data."), *available at* https://usa.visa.com/dam/VCOM/global/support-legal/documents/card-acceptance-guidelines-visa-merchants.pdf; MasterCard's "Security Rules and Procedures," Sept. 10, 2019, at p. 101 ("Compliance with the Payment Card Industry Data Security Standard is required for all . . . Merchants . . . that a Customer permits, directly or indirectly, to store, transmit, or process Account data."), *available at* https://www.mastercard.us/content/dam/mccom/en-us/documents/rules/SPME-Manual-September-2019.pdf.

279. Plaintiffs and Class members value data security and would not have provided their Card Information to Wawa in the absence of Wawa's implied promise to keep the Card Information reasonably secure.

280. Plaintiffs and Class members fully performed their obligations under their implied contracts with Wawa.

281. Wawa breached its implied contracts with Plaintiffs and Class members by failing to implement reasonable data security measures.

282. As a direct and proximate result of Wawa's breaches of the implied contracts, Plaintiffs and Class members sustained damages as alleged herein.

283. Plaintiffs and Class members are entitled to compensatory, consequential, and other damages suffered as a result of the Data Breach.

284. Plaintiffs and Class members are also entitled to injunctive relief requiring Wawa to, *inter alia*: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide several years of free credit monitoring and identity theft insurance to all Class members.

COUNT IV
UNJUST ENRICHMENT
(PLEADING IN THE ALTERNATIVE)
(On Behalf of the Nationwide Class or, in the Alternative, the State Classes)

285. Plaintiffs re-allege and incorporate by reference all allegations in paragraphs 1 through 232 as if fully set forth herein.

286. This claim is pleaded on behalf of Plaintiffs and the Nationwide Class or, in the alternative, the Delaware, Florida, Maryland, New Jersey, Pennsylvania, Virginia, and District of Columbia Classes pursuant to the common law of those jurisdictions.

287. This claim is pleaded in the alternative to Plaintiffs' claims for breach of implied contract in Count III, *supra*.

288. Plaintiffs and Class members conferred a monetary benefit upon Wawa in the form of monies paid for the purchase of food, fuel, other goods, and related services at Wawa's convenience store locations.

289. Wawa appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class members. Wawa also benefited from the receipt of Plaintiffs' and Class members' Card Information, as this was utilized by Wawa to facilitate payment to it.

290. The monies paid by Plaintiffs and Class members to Wawa were supposed to be used by Wawa, in part, to pay for adequate data security infrastructure, practices, and procedures.

291. As a result of Wawa's conduct, Plaintiffs and Class members suffered actual damages. For example, and not by way of limitation, Plaintiffs and Class members suffered benefit of bargain damages in an amount equal to the difference in value between their purchases if they had been protected by adequate data security for which Plaintiffs and Class members paid, and those purchases as actually received, *i.e.*, without adequate data security.

292. Wawa accepted and has retained these monetary benefits, and such acceptance and continued retention is inequitable and unjust. Because Wawa failed to implement (or adequately implement) data security practices that were otherwise mandated by the laws and industry standards alleged herein, principles of equity and good conscience militate against Wawa retaining the money belonging to Plaintiffs and Class members.

293. Wawa should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable proceeds that Wawa received as a result of its conduct and the Data Breach alleged herein.

COUNT V
VIOLATIONS OF THE DELAWARE CONSUMER FRAUD ACT
6 Del. Code §§ 2513, *et seq.*
(On Behalf of Plaintiffs Pierce, Russell, Tingle, and the Delaware Class)

294. Plaintiffs re-allege and incorporate by reference all allegations in paragraphs 1 through 232 as if fully set forth herein.

295. Wawa is a "person" involved in the "sale" of "merchandise" as each term is defined under 6 Del. Code §§ 2511(6)-(8).

296. Wawa advertised, offered, or sold goods or services in Delaware and engaged in trade or commerce directly or indirectly affecting the people of Delaware, including Plaintiffs and members of the Delaware Class.

297. Wawa used and employed deception, fraud, false pretense, false promise, misrepresentation, and concealment, suppression, and omission of material facts in connection with the sale and advertisement of merchandise, in violation of 6 Del. Code § 2513(a), including by:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Delaware Class members' Card Information, which failure was a direct and proximate cause of the Data Breach, and omitting, suppressing, and concealing the material fact of that failure;

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 failure was a direct and proximate cause of the Data Breach, and omitting, suppressing, and concealing the material fact of those failures;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Delaware Class members' Card Information, including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45, and Delaware's data security statute, 6 Del. Code § 12B-100 *et seq*., which failure was a direct and proximate cause of the Data Breach, and omitting, suppressing, and concealing the material fact of that failure;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Delaware Class members' Card 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' and Delaware Class members' Card Information, including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45, and Delaware's data security statute, 6 Del. Code § 12B-100 *et seq*.;

298. Wawa's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Wawa's data security and ability to protect the confidentiality of consumers' Card Information.

299. Wawa acted intentionally, knowingly, and maliciously to violate Delaware's Consumer Fraud Act, and recklessly disregarded Plaintiffs' and Delaware Class members' rights. Wawa's past data breaches alleged above, and the multitude of recent, similar malware-based payment card breaches, put it on notice that its security and privacy protections were inadequate.

300. Had Wawa disclosed to Plaintiffs and Delaware Class members that its data systems were not secure and, thus, were vulnerable to attack, customers would not have used

payment cards at Wawa or Wawa would have been forced to adopt reasonable data security measures and comply with the law.

301. Wawa's unlawful trade practices were gross, oppressive, and aggravated, and it breached the trust of Plaintiffs and Delaware Class members.

302. In addition, Wawa is a "person who conducts business in" Delaware "and owns, licenses, or maintains personal information," as defined by 6 Del. Code Ann. § 12B-101(6) & (7), and therefore is required to "implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business." 6 Del. Code Ann. § 12B-100.

303. As a person who conducts business in Delaware and owns or licenses computerized data that includes personal information, Wawa is required to "provide notice of any breach of security following determination of the breach of security to any resident of [Delaware] whose personal information was breached or is reasonably believed to have been breached" unless Wawa "reasonably determines" that the breach of security "is unlikely to result in harm to the individuals whose personal information has been breached." 6 Del. Code Ann. § 12B-102(a).

304. Because the Data Breach included or is reasonably believed to have included personal information, and because the breach was likely to, and did, result in misuse of the information and harm to individuals whose Card Information was breached, Wawa was required to accurately notify individuals (including Plaintiffs and Delaware Class Members) of the Data Breach, and to do so "without unreasonable delay" and no later than 60 days after Wawa had "sufficient evidence to conclude that a breach of security" had occurred. 6 Del. Code Ann. § 12B-102(a) and (c); 6 Del. Code Ann. § 12B-101(2).

305. Wawa's failure to implement and maintain reasonable procedures and practices to prevent the Data Breach and its failure to disclose the Data Breach in a timely and accurate manner constitute violations of the Delaware Consumer Fraud Act.

306. As a direct and proximate result of Wawa's unlawful acts and practices, Plaintiffs and Delaware Class members have suffered and will continue to suffer injury as described above, including 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; and increased, imminent risk of fraud and identity theft.

307. Plaintiffs and Delaware Class members seek all monetary and nonmonetary relief allowed by law, including damages under 6 Del. Code § 2525 for injury resulting from the direct and natural consequences of Wawa's unlawful conduct; punitive damages; injunctive relief; and/or reasonable attorneys' fees and costs.

COUNT VI
VIOLATIONS OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT,
Fla. Stat. § 501.201, *et seq*. ("FDUTPA")
(On Behalf of Plaintiffs McDaniel, Sussman, and the Florida Class)

308. Plaintiffs re-allege and incorporate by reference all allegations in paragraphs 1 through 232 as if fully set forth herein.

309. Plaintiffs and members of the Florida Class are "consumers" for purposes of Fla. Stat. § 501.203(7).

310. Plaintiffs and members of the Florida Class purchased "things of value" in the form of goods and services acquired from Wawa. Fla. Stat. § 501.203(9).

311. Wawa engaged in trade or commerce in Florida by advertising, soliciting, offering, providing, and entering into transactions intended to result, and which did result, in the sale of

goods, services, or things of value to consumers, including to Plaintiffs and members of the Florida Class. Fla. Stat.§ 501.203(8).

312. Wawa engaged in deceptive, unfair, and unlawful acts or practices in the conduct of trade or commerce in Florida, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

a. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Class members' Card Information, including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45, which failure was a direct and proximate cause of the Data Breach;

b. Representing that it maintained (when it failed to maintain) adequate data security practices to safeguard cardholder data such as the Card Information compromised in the Data Breach;

c. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Class members' Card Information;

d. Representing that its data security practices were adequate, while failing to disclose that its data security practices were inadequate to safeguard from theft cardholder data such as the Card Information compromised in the Data Breach;

e. 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' and Florida Class members' Card Information, including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45; and

f. Failing to timely and accurately disclose the Data Breach to Plaintiffs and the Florida Class members.

313. Wawa's conduct offends established public policy and is considered an unfair method of competition and constitutes unfair and unconscionable acts and practices. Fla. Stat. § 501.204(l).

314. Wawa's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Wawa's data security practices and ability to protect Card Information.

315. Wawa intended to mislead consumers and induce them to rely on its misrepresentations and omissions. Plaintiffs and Florida Class members did rely on Wawa's misrepresentations and omissions relating to Wawa's data privacy and security.

316. As a direct and proximate result of Wawa's violation of the FDUTPA, Plaintiffs and members of the Florida Class have suffered and will continue to suffer actual damages, injury, ascertainable losses of money or property, and monetary and non-monetary damages as set forth above, including, *inter alia*, paying a premium for Wawa's goods and services with the understanding that at least part of the premium would be applied toward sufficient and adequate data security practices that comply with industry standards, when in fact Wawa did not provide sufficient and adequate data security practices. Fla. Stat. § 501.211(2).

317. Also, as a direct result of Wawa's knowing violation of the FDUTPA, Plaintiffs and members of the Florida Class are entitled to not only actual damages, as described above, but also a declaratory judgment stating that Wawa's actions and practices alleged herein violate the FDUTPA. Fla. Stat. § 501.211(1).

318. Plaintiffs and members of the Florida Class are also entitled to injunctive relief requiring Wawa to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems; and (iii) provide several years of free credit monitoring and identity theft insurance to all class members. Fla. Stat. § 501.211(1).

319. Plaintiffs bring this action on behalf of themselves and members of the Florida Class for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect consumers from Wawa's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable, and unlawful practices.

320. Wawa's wrongful conduct as alleged in this Complaint has had a widespread impact on the public at large.

321. The above unfair and deceptive practices and acts by Wawa were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and members of the Florida Class that they could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

322. Wawa knew or should have known that its data security practices were inadequate to safeguard consumers' Card Information, and that the risk of a data theft was high.

323. Wawa's actions and inactions in engaging in the unfair practices and deceptive acts described herein were negligent, knowing and willful, and/or wanton and reckless.

324. Plaintiffs and members of the Florida Class seek relief under the FDUTPA, Fla. Stat. §§ 501.201, *et seq.*, including, but not limited to, damages, declaratory and injunctive relief, attorneys' fees and costs, and any other just and proper relief.

COUNT VII
VIOLATIONS OF THE MARYLAND CONSUMER PROTECTION ACT,
Md. Code Ann. Com. Law § 13-101, *et seq*.
(On Behalf of Plaintiffs Brulinski, Portnoy, and the Maryland Class)

325. Plaintiffs re-allege and incorporate by reference all allegations in paragraphs 1 through 232 as if fully set forth herein.

326. Wawa is a "person" as defined by Md. Code Ann. Com. Law § 13-101(h).

327. Wawa's conduct as alleged herein related to "sales" or "offers for sale" as defined by Md. Code Ann. Com. Law § 13-101(i) and § 13-303.

328. Plaintiffs and members of the Maryland Class are "consumers" as defined by Md. Code Ann. Com. Law § 13-101(c).

329. Wawa advertises, offers, or sells "consumer goods" or "consumer services" as defined by Md. Code Ann. Com. Law § 13-101(d).

330. Wawa advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting Maryland residents.

331. Wawa engaged in unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services, in violation of Md. Code Ann. Com. Law § 13-303 by, among other things:

a. Failing to implement and maintain reasonable data security measures to protect consumers' Card Information, which failure was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks;

c. Failing to remediate identified security and privacy risks;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of consumers' Card Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

e. Misrepresenting that it would protect the privacy of consumers' Card Information, including by implementing and maintaining reasonable security measures;

f. Omitting, suppressing, and concealing the material fact that it did not adequately secure consumers' Card 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 of consumers' Card Information.

332. Wawa's misrepresentations and omissions were material because they were likely to deceive reasonable consumers (including Plaintiffs and members of the Maryland Class) about the adequacy of Wawa's data security and ability to protect Card Information. Wawa's misrepresentations and omissions were important to a significant number of consumers (including Plaintiffs and members of the Maryland Class) in making decisions to use payment cards at Wawa's convenience stores.

333. Wawa intended to mislead Plaintiffs and members of the Maryland Class and induce them to rely on its misrepresentations and omissions.

334. If Plaintiffs and members of the Maryland Class had known the truth about Wawa's data security practices and its failure to adequately protect Card Information, they would not have used their payment cards at Wawa stores, or would have paid less for goods and services purchased from Wawa.

335. Wawa acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded the rights of consumers.

336. Wawa's above-described wrongful actions and omissions directly and/or proximately resulted in the various types of harm to Plaintiffs and members of the Maryland Class identified in detail above.

337. Further, under the Maryland Personal Information Protection Act, "[t]o protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of personal information owned or licensed and the nature and size of the business and its operations." Md. Comm. Code § 14-3503(a).

338. Wawa is a business as defined by Md. Comm. Code § 14-3501(b)(1).

339. Plaintiffs' and Maryland Class members' personal Card Information includes personal information as covered under Md. Comm. Code § 14-3501(e).

340. In violation of Md. Comm. Code § 14-3503, Wawa did not maintain reasonable data security procedures and practices appropriate to the nature of the personal information it owned, maintained, or licensed and the nature and size of its business and operations.

341. The Data Breach was a "breach of the security of a system" as defined by Md. Comm. Code § 14-3504(a).

342. Under Md. Comm. Code § 14-3504(b)(1), "[a] business that owns, licenses, or maintains computerized data that includes personal information of an individual residing in the State, when it discovers or is notified that it incurred a breach of the security of a system, shall

conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach."

343. Under Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), "if, after the investigation is concluded, the business determines that the breach of the security of the system creates a likelihood that personal information has been or will be misused, the owner or licensee of the computerized data shall notify the individual of the breach" and that notification "shall be given as soon as reasonably practical, but not later than 45 days after the business discovers or is notified of the breach of the security of a system."

344. Because Wawa discovered and had notice of a security breach, Wawa had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

345. By failing to disclose the Data Breach in a timely and accurate manner, Wawa violated Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

346. As a direct and proximate result of Wawa's violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), Plaintiffs and Maryland Class members suffered damages, as described above.

347. Pursuant to Md. Comm. Code § 14-3508, Wawa's violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the Maryland Consumer Protection Act, 13 Md. Comm. Code §§ 13-101 *et seq.*, and are subject to the enforcement and penalty provisions contained within the Maryland Consumer Protection Act.

348. Plaintiffs and Maryland Class members seek relief under Md. Comm. Code §13-408 for the injuries and losses they have sustained as the result of Wawa's violation of the Maryland Personal Information Protection Act and Consumer Protection Act.

349. Plaintiffs and members of the Maryland Class seek all monetary and non-monetary relief allowed by law, including actual and consequential damages, restitution, disgorgement, injunctive relief, and/or attorneys' fees and costs.

COUNT VIII
VIOLATIONS OF THE NEW JERSEY CONSUMER FRAUD ACT,
N.J. Stat. Ann. §§ 56:8-1, *et seq.* ("NJCFA")
(On Behalf of Plaintiffs Bruno, Muller, and the New Jersey Class)

350. Plaintiffs re-allege and incorporate by reference all allegations in paragraphs 1 through 232 as if fully set forth herein.

351. Plaintiffs and New Jersey Class members used their credit or debit cards to purchase convenience store items and fuel from Wawa locations in New Jersey.

352. Wawa engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of "merchandise" as defined by N.J. Stat. Ann. § 56:8-1.

353. Wawa is engaged in, and its acts and omissions affect, trade and commerce. Wawa's relevant acts, practices, and omissions complained of in this action were conducted in the course of Wawa's business of marketing, offering for sale, and selling food products, fuel, goods, and services throughout the state of New Jersey and the eastern United States.

354. N.J. Stat. Ann. 56:8-2 (the "NJCFA") prohibits the "act, use or employment by any person of any unconscionable commercial practice, 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."

355. In the conduct of its business, trade, and commerce, and in the sale of food products, fuel, goods, or services to consumers in the state of New Jersey, Wawa collected and stored highly personal and private information, including sensitive Card Information of Wawa's customers, including Plaintiffs and the New Jersey Class members.

356. Wawa knew or should have known that its computer systems and data security practices were inadequate to safeguard customers' sensitive Card Information and that there was a high risk of a data breach.

357. Wawa should have disclosed this information regarding its inadequate data security practices because Wawa was in a superior position to know the true facts related to its security vulnerabilities, and Plaintiffs and members of the New Jersey Class could not reasonably be expected to learn or discover those true facts.

358. Wawa intended to mislead customers, including Plaintiffs and members of the New Jersey Class, and induce them to rely on its misrepresentations and omissions. Had Plaintiffs and members of the New Jersey Class known of Wawa's inadequate data security practices and Wawa's vulnerability to attack, they would not have given their Card Information to Wawa.

359. Wawa's representations and omissions were material because they were likely to deceive reasonable customers about the adequacy of Wawa's data security practices and ability to protect Card Information.

360. As alleged herein, Wawa engaged in unconscionable, deceptive, unfair, and unlawful acts or practices in the conduct of trade or commerce and the sale of food products, fuel,

goods, or services to customers in the state of New Jersey, in violation of the NJCFA, including but not limited to by:

a. Failing to adequately secure the sensitive financial information of Plaintiffs and members of the New Jersey Class;

b. Failing to maintain adequate computer systems and data security practices to safeguard customers' personal and financial information;

c. Misrepresenting the material fact that Wawa would maintain adequate data privacy and security practices and procedures to safeguard customer's sensitive financial information from unauthorized disclosure, release, data breaches, and theft;

d. Misrepresenting that Wawa did and would comply with the requirements of relevant federal and state laws and industry standards pertaining to the privacy and security of the sensitive financial information of Plaintiffs and members of the New Jersey Class;

e. Knowingly omitting, suppressing, and concealing the material fact that Wawa's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft, with the intent that others rely upon the omission, suppression, and concealment;

f. Failing to disclose in a timely and accurate manner to Plaintiffs and members of the New Jersey Class the material fact of the nature and extent of the Data Breach; and

g. Continuing to accept credit and debit card payments and store Card Information after Wawa knew or should have known of the data breach and before Wawa allegedly remedied the breach.

361. Wawa's actions in engaging in the conduct above were negligent, knowing, willful, wanton, and/or reckless with respect to the rights of Plaintiffs and members of the New Jersey Class.

362. As a direct and proximate result of Wawa's violation of the NJCFA, Plaintiffs and members of the New Jersey Class have suffered injury as described above, including ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; loss of use of account funds; expenditure of time and money to access, monitor, and correct financial accounts; and increased, imminent risk of fraud and identity theft.

363. Further, Wawa is a business that compiles or maintains computerized records that include personal information covered under N.J. Stat. Ann. §§ 56:8-161, *et seq*.

364. Under N.J. Stat. Ann. § 56:8-163(a), "[a]ny business that conducts business in New Jersey . . . shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay . . . ."

365. Because Wawa discovered a breach of its computer systems in which personal information was, or is reasonably believed to have been, acquired by an unauthorized person, and the personal information was not secured by encryption or otherwise, Wawa had an obligation to disclose the Wawa Data Breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. § 56:8-163, *et seq.*

366. By failing to disclose the Wawa Data Breach in a timely and accurate manner, Wawa violated N.J. Stat. Ann. § 56:8-163(a).

367. Pursuant to N.J. Stat. Ann. § 56:8-166, Wawa's violation of N.J. Stat. Ann. § 56:8-163 constitutes a violation of the NJCFA, and is enforceable through N.J. Stat. Ann. § 56:8-19.

368. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiffs and New Jersey Class members seek relief under N.J. Stat. Ann. § 56:8-19, including but not limited to actual damages, treble damages, injunctive relief, and attorneys' fees and costs.

369. Pursuant to N.J. Stat. Ann. § 56:8-20, this Complaint will be served upon the New Jersey Attorney General.

COUNT IX
VIOLATIONS OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW
73 Pa. Stat. §§ 201-1 to 201-9.2 ("UTPCPL")
(On Behalf of Plaintiffs Graziano, Rolling, and the Pennsylvania Class)

370. Plaintiffs re-allege and incorporate by reference all allegations in paragraphs 1 through 232 as if fully set forth herein.

371. Plaintiffs and Wawa are "persons" as defined at 73 Pa. Stat. § 201-2(2).

372. Plaintiffs and Pennsylvania Class members purchased goods and services in "trade" and "commerce" as defined at 73 Pa. Stat. § 201-2(3).

373. Plaintiffs and Pennsylvania Class members purchased goods and services primarily for personal, family, and/or household purposes under 73 Pa. Stat. § 201-9.2.

374. Wawa engaged in "unfair methods of competition" or "unfair or deceptive acts or practices" as defined at 73 Pa. Stat. § 201-2(4) by, among other things, engaging in the following conduct:

a. Representing that its goods and services had characteristics, uses, benefits, and qualities that they did not have – namely that its goods, services, and business practices were accompanied by adequate data security (73 Pa. Stat. § 201-2(4)(v));

b. Representing that its goods and services were of a particular standard or quality when they were of another standard or quality (73 Pa. Stat. § 201-2(4)(vii));

c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. § 201-2(4)(ix); and

d. "Engaging in any other … deceptive conduct which creates a likelihood of confusion or of misunderstanding" (73 Pa. Stat. § 201-2(4)(xxi)).

375. These unfair methods of competition and unfair or deceptive acts or practices are declared unlawful by 73 Pa. Stat. § 201-3.

376. Wawa's unfair or deceptive acts and practices include but are not limited to: failing to implement and maintain reasonable data security measures to protect Card Information; failing to identify foreseeable data security risks and remediate the identified risks; failing to comply with common law duties, industry standards including PCI DSS, and FTC guidance regarding data security; misrepresenting in its Privacy Policy that it would protect cardholder data such as the Card Information compromised in the Data Breach; and omitting and concealing the material fact that it did not have reasonable measures in place to safeguard such Card Information.

377. Wawa's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Wawa's data security practices and ability to protect Card Information.

378. Wawa intended to mislead consumers and induce them to rely on its misrepresentations and omissions. Plaintiffs and Pennsylvania Class members did rely on Wawa's misrepresentations and omissions relating to its data privacy and security.

379. Plaintiffs and Pennsylvania Class members acted reasonably in relying on Wawa's misrepresentations and omissions, the truth of which they could not have discovered with reasonable diligence.

380. Had Wawa disclosed to consumers that its data security systems were not secure and, thus, were vulnerable to attack, Plaintiffs and class members would not have given their Card Information to Wawa.

381. Wawa acted intentionally, knowingly, and maliciously in violating the Pennsylvania UTPCPL, and recklessly disregarded consumers' rights.

382. Wawa's past payment card data breaches put it on notice of the importance of data security and that its card processing system was subject to attack.

383. As a direct and proximate result of Wawa's unfair methods of competition and unfair or deceptive acts or practices, Plaintiffs and Pennsylvania Class members have suffered and will continue to suffer damages, injury, ascertainable losses of money or property, and monetary and non-monetary damages as described above.

384. Plaintiffs and Pennsylvania Class members seek all monetary and non-monetary relief allowed by law, including the following as expressly permitted under 73 Pa. Stat. § 201-9.2:

a. "actual damages or [statutory damages of] one hundred dollars ($100), whichever is greater";

b. treble damages, defined as "three times the actual damages";

c. "reasonable attorney fees" and litigation costs; and

d. "such additional relief as [the Court] deems necessary or proper."

385. Plaintiffs and Pennsylvania Class members also seek the injunctive relief as set forth above.

COUNT X
VIRGINIA CONSUMER PROTECTION ACT,
Va. Code Ann. §§ 59.1-196, *et seq.*
(On Behalf of Plaintiff Garthwaite and the Virginia Class)

386. Plaintiffs reallege and incorporate by reference all allegations in paragraphs 1 through 232 as if fully set forth herein.

387. The Virginia Consumer Protection Act prohibits "[u]sing any … deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

388. Wawa is a "person" and "supplier" as defined by Va. Code Ann. § 59.1-198.

389. Wawa engaged in the complained-of conduct in connection with "consumer transactions" with regard to "goods" and "services," as defined by Va. Code Ann. § 59.1-198. Wawa advertised, offered, or sold goods or services to be used primarily for personal, family or household purposes.

390. Wawa intended to mislead consumers and induce them to rely on its misrepresentations and omissions. Plaintiff and Virginia Class members did rely on Wawa's misrepresentations and omissions relating to Wawa's data privacy and security.

391. Wawa engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, including:

a. Failing to implement and maintain reasonable data security measures to protect Plaintiff and Virginia Class members' Personal Information, which failure was a

direct and proximate cause of the Data Breach, but falsely pretending and misrepresenting that its data security and privacy measures were adequate;

b. Failing to identify foreseeable data security risks, remediate identified data security risks, and adequately improve data security measures following previous cybersecurity incidents, which failure was a direct and proximate cause of the Data Breach, but falsely pretending and misrepresenting that it adequately protected Cardholder Information;

c. Failing to comply with common law and statutory duties pertaining to the security of Plaintiff and Virginia Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which failure was a direct and proximate cause of the Data Breach, but falsely pretending and misrepresenting that it complied with its legal duties;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Virginia Class members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the data security of Plaintiff and Virginia Class members' Personal 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 adequately secure Plaintiff and Virginia Class members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the data security of Plaintiff

and Virginia Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45. Wawa intended to mislead Plaintiff and Virginia Class members and induce them to rely on its misrepresentations and omissions.

392. Wawa's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and Virginia Class members, about the adequacy of Wawa's data security and the quality of the Wawa brand.

393. Had Wawa disclosed to Plaintiff and Virginia Class members that its data systems were not secure and thus were vulnerable to attack, Wawa 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, Wawa received, maintained, and compiled Plaintiff's and Virginia Class members' Confidential Information as part of the services Wawa provided, and for which Plaintiff and Virginia Class members paid, without advising Plaintiff and Virginia Class members that Wawa's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff's and Virginia Class members' Card Information. Accordingly, Plaintiff and the Virginia Class members acted reasonably in relying on Wawa's misrepresentations and omissions, the truth of which they could not have discovered.

394. Wawa had a duty to disclose these facts due to the circumstances of the breach and the sensitivity and extent of the Personal Information in its possession. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Virginia Class —and Wawa, because consumers are unable to fully protect their interests with regard to their data, and they placed trust and confidence in Wawa. Wawa's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its data security; and/or

c. Incomplete representations about the security and integrity of its card processing systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Virginia Class that contradicted these representations.

395. The above-described deceptive acts and practices also violated the following provisions of VA Code § 59.1-200(A):

a. Misrepresenting that goods or services have certain quantities, characteristics, ingredients, uses, or benefits;

b. Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model; and

c. Advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised.

396. Wawa acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act, and recklessly disregarded Plaintiff and Virginia Class members' rights. Wawa's past data breaches and prior breaches within the retail industry put Wawa on notice that its data security processes were inadequate. An award of punitive damages would serve to punish Wawa for its wrongdoing, and warn or deter others from engaging in similar conduct.

397. As a direct and proximate result of Wawa's deceptive acts or practices, Plaintiff and Virginia Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages as described above. Such injuries, losses, and damages include loss of the benefit of the bargain with Wawa as Plaintiffs would not

have paid Wawa for goods and services or would have paid less for such goods and services but for Wawa's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring financial accounts for fraudulent activity; time and money spent canceling and replacing payment cards; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

398. Wawa's violations present a continuing risk to Plaintiff and Virginia Class members, as well as to the general public.

399. Plaintiff and Virginia Class members seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages in the amount of $1,000 per violation if the conduct is found to be willful or, in the alternative, $500 per violation; restitution; injunctive relief; punitive damages; and attorneys' fees and costs.

COUNT XI
VIOLATION OF THE VIRGINIA PERSONAL INFORMATION BREACH NOTIFICATION ACT, Va. Code. Ann. §§ 18.2-186.6
(On Behalf of Plaintiff Garthwaite and the Virginia Class)

400. Plaintiffs re-allege and incorporate by reference all preceding allegations in paragraph 1 through 232 as if fully set forth herein.

401. Under Va. Code Ann. § 18.2-186.6(B), Wawa is required to accurately and promptly notify Plaintiff and Virginia Class Members following discovery of a breach of its payment card processing system if unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person which causes or is reasonably believed to cause identify theft or another fraud to any resident of Virginia

402. Plaintiff's and Virginia Class members' Payment Card Information includes Personal Information as defined by Va. Code Ann. § 18.2-186.6(A).

403. Because Wawa discovered a breach of its payment card processing system in which Wawa stored Plaintiff's and Virginia Class members' unencrypted or unredacted Payment Card Information that 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, Wawa 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).

404. By failing to disclose the Data Breach in a timely and accurate manner, Wawa violated Va. Code Ann. § 18.2-186.6(B).

405. Wawa's above-described wrongful actions, inaction, and omissions, unconscionable, unfair, and deceptive acts or practices, failure to timely and accurately disclose the Data Breach, and failure to use reasonable measures to safeguard, protect, and monitor the security of Plaintiff's and Virginia Class members' Card Information, directly and/or proximately resulted in injury, harm, and damages to Plaintiffs and Virginia Class members as set forth above and in the form of, *inter alia*, the ongoing, imminent, and impending threat of identity theft and identity fraud; actual identity theft and identity fraud; loss of the confidentiality of the wrongfully disclosed and compromised Card Information; the illegal sale of the compromised Card Information on the dark web; lost value of the compromised Card Information; cost of monitoring, credit freezes, and/or identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports, and repairing damaged credit; expenses and/or time spent initiating fraud alerts; decreased credit scores and credit ratings; lost work time; and other economic and non-economic injury, harm, and damages.

406. Wawa's above-described wrongful actions, inactions, and omissions constitute breaches of the Virginia Personal Information Breach Notification Act.

407. Plaintiff and Virginia Class members seek all monetary and non-monetary relief allowed by law, including direct economic damages, injunctive relief, and attorneys' fees and costs, and all other relief the Court deems proper.

COUNT XII
VIOLATION OF THE DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT
D.C. Code §§ 28-3901, *et seq.* ("D.C. CPPA")
(On Behalf of Plaintiff Lucas and the District of Columbia Class)

408. Plaintiffs re-allege and incorporate by reference all preceding allegations in paragraphs 1 through 232 as if fully set forth herein.

409. Wawa is a "person," Plaintiff and the District of Columbia ("D.C.") Class members are "consumers," and Wawa offered for sale "goods and services," as those terms are defined under D.C. Code §§ 28-3901(a)(1), (2), and (7).

410. Plaintiff and D.C. Class members purchased goods and services from Wawa for personal, household, or family purposes.

411. As set forth herein, Wawa failed to protect Plaintiff's and D.C. Class members' Card Information due to data security failures, and misrepresented or omitted the nature of its inadequate data security policies and procedures.

412. Wawa's conduct and acts alleged herein constitute unfair or deceptive trade practices in violation of the D.C. Code § 28-3904 in at least the following ways:

a. Failing to implement and maintain reasonable data security measures to protect Plaintiff's and D.C. Class members' Card Information, which failure was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable data security risks, remediate identified data security risks, and adequately improve data security measures following previous cybersecurity incidents, which failure was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the data security of Plaintiff's and D.C. Class members' Card Information, including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45, and D.C. Code §§ 28-3851 through 2853, the D.C. Consumer Security Breach Notification Act ("D.C. CSBNA"), which failure was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and D.C. Class members' Card Information, including by implementing and maintaining reasonable data security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the data security of Plaintiff's and D.C. Class members' Card Information, which includes duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45, and the D.C. CSBNA, D.C. Code §§ 28-3851 through 2853;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and D.C. Class members' Card Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the data security of Plaintiff's and D.C. Class members' Card Information, including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45, and the D.C. CSBNA, D.C. Code §§ 28-3851 through 28-5383.

413. Wawa intended to mislead consumers and induce them to rely on its misrepresentations and omissions. Plaintiffs and D.C. Class members did rely on Wawa's misrepresentations and omissions relating to Wawa's data security.

414. Wawa's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Wawa's data security and ability to protect the confidentiality of consumers' Card Information, and because a significant number of unsophisticated consumers would find information about the inadequacy of Wawa's data security important in determining a course of action.

415. Wawa acted intentionally, knowingly, and maliciously to violate the D.C. Consumer Protection Procedures Act, and recklessly disregarded Plaintiff's and D.C. Class members' rights. Wawa's past data breaches, discussed *supra*, and the multitude of recent, similar malware-based payment card breaches put Wawa on notice that its security and privacy protections were inadequate.

416. Had Wawa disclosed to Plaintiff and D.C. Class members that its payment card systems were not secure and thus were vulnerable to attack, Wawa would have been forced to adopt reasonable data security measures and comply with the law. Instead, it held itself out as a company that values data privacy, and it was entrusted with sensitive and valuable Card Information for millions of consumers, including Plaintiff and the D.C. Class members. Plaintiff and the D.C. Class members acted reasonably in providing their Card Information to Wawa, and were injured by Wawa's misrepresentations and omissions, the truth of which they could not have discovered.

417. Wawa's unlawful trade practices were gross, oppressive, and aggravated, and Wawa breached the trust of Plaintiff and the D.C. Class members.

418. As a direct and proximate result of Wawa's unlawful acts and practices, Plaintiff and D.C. Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages as set forth above, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; and increased, imminent risk of fraud and identity theft.

419. Plaintiff and D.C. Class members seek all monetary and nonmonetary relief allowed by law, including the greater of $1,500 per violation or treble damages for injury resulting from the direct and natural consequences of Wawa's unlawful conduct; injunctive relief; punitive damages; reasonable attorneys' fees and costs; and all other relief the Court deems proper.

COUNT XIII
VIOLATION OF THE DISTRICT OF COLUMBIA CONSUMER SECURITY BREACH NOTIFICATION ACT, D.C. Code §§ 28-3851, *et seq.*[61]
(On Behalf of Plaintiff Lucas and the District of Columbia Class)

420. Plaintiffs re-allege and incorporate by reference all preceding allegations in paragraphs 1 through 232 as if fully set forth herein.

421. Wawa is a "person or entity who conducts business in the District of Columbia, and who, in the course of such business, owns or licenses computerized or other electronic data that includes personal information." D.C. Code § 28-3852(a).

422. Plaintiff's and D.C. Class Members' Card Information includes "personal information" as defined by D.C. Code § 28-3851(3).

[61] The D.C. Consumer Security Breach Notification Act ("DC CSBNA") was amended by 2020 District of Columbia Laws 23-98 (Act 23-268), effective June 17, 2020. Plaintiffs cite the statute as it was in effect at the time of the Data Breach.

423. The D.C. CSBNA required Wawa to accurately notify Plaintiffs and Class Members of the Data Breach when Wawa discovered it, and to do so in the most expedient time possible without unreasonable delay. D.C. Code § 28-3852(a).

424. Because Wawa was aware of the breach of its payment card processing system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by D.C. Code § 28-3852(a).

425. By failing to disclose the Data Breach in a timely and accurate manner, however, Wawa violated D.C. Code § 28-3852(a).

426. Wawa's above-described wrongful actions, inactions, and omissions, failure to timely and accurately report the Data Breach, and failure to use reasonable measures to safeguard, protect, and monitor the security of Plaintiff's and D.C. Class members' Card Information directly and/or proximately resulted in injury, harm, and damages to Plaintiff and D.C. Class Members as set forth above.

427. Wawa's above-described wrongful actions, inactions, and omissions constitute violations of the District of Columbia Consumer Security Breach Notification Act.

428. Plaintiff and D.C. Class members seek all monetary and nonmonetary relief allowed by law, including actual damages, injunctive relief, the costs of the action, and reasonable attorney's fees, and all other relief the Court deems proper.

VII. RELIEF REQUESTED

Plaintiffs, on behalf of themselves and all others similarly situated, request that the Court enter judgment against Wawa including as follows:

A. Determining that this matter may proceed as a class action and certifying the Classes alleged herein;

B. Appointing Plaintiffs as representatives of the applicable Classes, and appointing Plaintiffs' counsel as class counsel on behalf of the Certified Class or Classes;

C. Granting an award to Plaintiffs and the Classes of compensatory, consequential, statutory, punitive, treble, and all other damages allowed by law;

D. Ordering injunctive relief requiring Wawa to, *inter alia:* (i) strengthen its data security systems and monitoring procedures to prevent further breaches; (ii) submit to future annual audits of those systems; and (iii) provide several years of free credit monitoring and identity theft insurance to all class members;

E. Granting an award of attorneys' fees, costs, and expenses, as provided by law or equity;

F. Granting an award of pre-judgment and post-judgment interest, as provided by law or equity; and

G. Granting such other relief as the Court may allow.

VIII. JURY TRIAL DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

Dated: July 27, 2020

Respectfully submitted,

/s/ Benjamin F. Johns

Benjamin F. Johns (PA Bar No. 201373)
Samantha E. Holbrook (PA Bar No. 311829)
Andrew W. Ferich (PA Bar No. 313696)
Mark B. DeSanto (PA Bar No. 320310)
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
Tel: (610) 642-8500
bfj@chimicles.com

seh@chimicles.com
awf@chimicles.com
mbd@chimicles.com

Sherrie R. Savett (PA Bar No. 17646)
Jon J. Lambiras (PA Bar No. 92384)
BERGER MONTAGUE, PC
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Tel: (215) 875-3000
Fax: (215) 875-4604
ssavett@bm.net
jlambiras@bm.net

Roberta D. Liebenberg (PA Bar No. 31738)
Gerard A. Dever (PA Bar No. 85291)
Mary L. Russell (PA Bar No. 58581)
FINE, KAPLAN AND BLACK, R.P.C.
One South Broad St., 23rd Floor
Philadelphia, PA 19107
Tel: (215) 567-6565
rliebenberg@finekaplan.com
gdever@finekaplan.com
mrussell@finekaplan.com

Linda P. Nussbaum
Bart Cohen (PA Bar No. 57606)
NUSSBAUM LAW GROUP, P.C.
1211 Avenue of the Americas, 40th Fl.
New York, NY 10036-8718
Tel: (917) 438-9102
lnussbaum@nussbaumpc.com
bcohen@nussbaumpc.com

Interim Co-Lead Class Counsel for the Consumer Track

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on July 27, 2020, a true and correct copy of the above and foregoing was filed with the Clerk of Court via the Court's CM/ECF system for electronic service on all counsel of record.

Dated: July 27, 2020

By: */s/ Benjamin F. Johns*
Benjamin F. Johns