UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

JOSEPH MULLER, on behalf of himself and all others similarly situated, Plaintiff, vs. WAWA, INC., Defendant.	Case No. _____ Civil Action **COMPLAINT - CLASS ACTION**

Plaintiff Joseph Muller ("Plaintiff"), on behalf of himself and all others similarly situated, brings this class action complaint against defendant Wawa, Inc. ("Wawa" or "Defendant"). Plaintiff alleges as follows upon personal knowledge as to his own acts and experience, and upon the investigation of his attorneys as to all other matters.

I. INTRODUCTION

1. This is a data breach class action on behalf of millions of consumers whose credit and debit card numbers were stolen by a computer hacker in a cyber-attack involving Wawa. The data breach involved consumer transactions at all or most of Wawa's 850 convenience stores over a nine-month period. Information compromised in the breach consists of consumers' credit and debit card numbers, card expiration dates, and cardholder names. The hacker stole card information from Defendant's servers from March 4, 2019 to December 12, 2019 (the "Data Breach").

2. As a result of the Data Breach, many class members have experienced and will continue to experience fraudulent credit or debit card purchases. Class members will also incur out-of-pocket costs to purchase protective measures such as credit monitoring services, credit

freezes, and credit reports. They will also incur costs for replacement cards or other items directly or indirectly related to the Data Breach.

3. Plaintiff and class members have been exposed to a heightened and imminent risk of fraud and identity theft. 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.

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

II. PARTIES

5. Plaintiff Joseph Muller is a resident of New Jersey. He used his debit card on dozens of occasions at multiple Wawa locations in New Jersey throughout the breach period. After using his debit card at Wawa, he suffered fraudulent purchases on the same card on multiple occasions. One such fraudulent purchase took place in or around July 2019. His bank reversed the charge and issued him a replacement card. He used that new card at Wawa on multiple occasions. He then suffered a fraudulent charge on the new card in or around September 2019, for approximately $60. Plaintiff Muller's bank again reversed the charge and issued him a replacement card. He again used that new card at Wawa on multiple occasions. He then suffered a fraudulent transaction on that card on December 9, 2019, totaling approximately $400. Plaintiff Muller's bank reversed the fraudulent charge and issued him a replacement card. Each time his card was re-issued, Plaintiff Muller had to wait several days for the new card to be issued and he had no convenient way to access his bank account funds in the meantime. He also

spent time re-establishing payment links to his new card number each time the card was re-issued. To Plaintiff Muller's knowledge, the fraud on his card was likely related to the Wawa breach. His purchases at Wawa were a common link to each successive card that experienced fraud. To his knowledge, his debit card number was not involved in any other data breaches other than the Wawa breach.

6. Defendant Wawa, Inc. is a privately held company with its principal place of business in Wawa, Pennsylvania. It is incorporated in New Jersey. It operates 850 convenience stores in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida, and Washington, D.C. It employs over 35,000 individuals and has annual revenue over $10 billion.

III. JURISDICTION AND VENUE

7. 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 Defendant.

8. This Court has personal jurisdiction over Defendant because Defendant conducts business in and throughout Pennsylvania, and the wrongful acts alleged in the Complaint were committed largely in Pennsylvania.

9. 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 Plaintiff's claims occurred in this District. Venue is also proper pursuant to 28 U.S.C. § 1391(b)(1) because Defendant is headquartered in this District and is a resident for venue purposes because it regularly transacts business here. Further, venue is proper under 28 U.S.C. § 1391(b)(3) because Defendant is subject to personal jurisdiction in this District.

IV. FACTUAL ALLEGATIONS

10. Defendant is an operator of a large chain of convenience stores and gas stations.

11. On December 19, 2019, Defendant publicly announced the Data Breach, stating the following on its website:

> 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 April 22, 2019, however, some locations may not have been affected at all. No other personal information was accessed by this malware. . . .[1]

12. Defendant also noted that the malware "may have captured some information about Wawa gift card numbers."[2]

---

[1] https://www.wawa.com/alerts/data-security, Notice tab (emphasis added) (last visited Dec. 21, 2019).

[2] https://www.wawa.com/alerts/data-security, Frequently Asked Questions tab (last visited Dec. 21, 2019).

13. Defendant disclosed 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.[3] However, thieves reportedly can still make fraudulent purchases without access to the security code:

> [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 code has only 999 possible answers, after all. "That sounds like lot to human," he says. "To a machine, it's nothing."[4]

14. Defendant failed to properly safeguard class members' card information, allowing the hacker to access credit and debit card information for months. Defendant also failed to properly monitor its systems. Had it properly monitored its care payment systems, it would have discovered the malware much sooner than nine months after the breach began.

15. Defendant had a duty pursuant to common law, industry standards, card network rules, and representations made in its own privacy policy to keep consumers' card information confidential and to protect it from unauthorized access.

16. Defendant's Privacy Policy stated 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 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. . . .

---

[3] https://www.wawa.com/alerts/data-security, Notice tab (last visited Dec. 21, 2019).

[4] *The Wawa Credit Card Breach: What You Need to Know*, Philadelphia Magazine, Dec. 20, 2019, *available at* https://www.phillymag.com/news/2019/12/20/wawa-data-breach/.

. . . .

Data Security

Wawa is fully committed to data security.[5]

17. Plaintiff and class members provided their card information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep the card information confidential and would secure it from unauthorized access.

18. Defendant's data security obligations were particularly important and well-known to Defendant given the substantial increase in payment card data breaches throughout the retail industry preceding the Data Breach. The increase in data breaches, and the risk of future breaches, was widely known throughout the retail industry, including to Defendant.

19. The Pennsylvania Attorney General has initiated an investigation into the Data Breach.[6]

A. Defendant's Data Security Failures

20. Defendant breached its duties, obligations, and promises by not:

a. Adequately safeguarding consumers' credit and debit card information;

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

c. Properly monitoring its data security systems for existing intrusions and weaknesses;

[5] https://www.wawa.com/privacy (last visited Dec. 21, 2019).

[6] https://www.law360.com/retail/articles/1230186/wawa-data-breach-exposed-credit-debit-card-numbers.

d. Performing penetration tests to determine the strength of its credit and debit card processing systems;

e. Properly training its information technology staff on matters relevant to cardholder data security; and

f. Retaining outside vendors to periodically test its credit card processing systems.

i. Defendant Violated PCI Data Security Standards

21. 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 including Defendant must take to ensure that payment card information is properly safeguarded.

22. The payment card networks (primarily MasterCard, Visa, American Express, and Discover) have issued card operating rules that are binding on merchants including Defendant and require merchants to protect cardholder data. In particular, the Payment Card Industry Security Standards Council promulgates minimum standards that apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Industry Data Security Standards ("PCI DSS"). PCI DSS is the industry standard governing the security of credit and debit card data.

23. PCI DSS establishes detailed comprehensive requirements for satisfying each of the following 12 "high-level" mandates:[7]

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

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

24. As noted in the chart, PCI DSS required Defendant to "protect all systems against malware." Defendant failed to do so. Defendant specified that the hacker placed "malware" on Defendant's payment processing servers.

25. PCI DSS also required Defendant to "[t]rack and monitor all access to network resources." Defendant failed to do so. The hacker had access to Defendant's system for nine months, illustrating that Defendant had materially deficient tracking and monitoring systems in place.

26. On information and belief, Defendant violated numerous other provisions of the PCI DSS, including subsections underlying the chart above. Those deficiencies will be revealed during discovery with the assistance of expert witnesses.

27. PCI DSS sets the minimum level of what must be done, not the maximum. While PCI compliance is an important first step in securing cardholder data, it is not sufficient on its own to protect against all breaches, nor does it provide a safe harbor against civil liability for a data breach.

28. At all relevant times, Defendant was well-aware of its PCI DSS obligations to protect cardholder data. Defendant was an active participant in the payment card networks as it collected and transmitted millions of sets of payment card data per day.

ii. Defendant Violated the FTC Act

29. The Federal Trade Commission ("FTC") 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 Federal Trade Commission Act ("FTCA"), 15 U.S.C. §45.

30. The FTC published guidance establishing reasonable data security practices for businesses. The FTC guidance notes that businesses should, *e.g.*: protect the personal customer information that they acquire; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security vulnerabilities. FTC guidance also recommends that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating that someone may be trying to penetrate the system; and watch for large amounts of data being transmitted from the system.[8]

31. 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.

---

[8] *See, e.g., Start with Security: A Guide for Business*, Federal Trade Commission, June 2015, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf; *Protecting Personal Information: A Guide for Business*, Federal Trade Commission, Oct. 2016, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

32. Defendant knew or should have known about its obligation to comply with the FTC Act regarding data security.

33. Defendant's misconduct violated the FTC Act, led to the Data Breach, and caused harm to Plaintiff and class members.

B. Defendant's Data Breach History

34. Wawa has a history of credit card intrusions.

35. 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.[9]

36. Similarly, in 2018, police investigated a skimming device placed on a Wawa gas pump, which reportedly led to fraudulent credit card purchases.[10]

37. These breaches put Defendant 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, Defendant nevertheless failed to adopt adequate data security governing its credit and debit card transactions.

C. Damages to Class Members

38. Plaintiff and class members have been damaged by the compromise of their card information in the Data Breach.

---

[9] https://privacyrights.org/data-breaches (Excel spreadsheet describing data breaches).

[10] *Police Investigating Credit Fraud Related to Wawa*, Northeast Times, May 24, 2018, *available at* https://northeasttimes.com/2018/05/24/police-investigating-credit-fraud-related-to-wawa/.

39. Class members face a substantial and imminent risk of fraudulent charges on their credit and debit cards. The hacker stole the card information with the intent to use it for fraudulent purposes and/or to sell it on the dark web.

40. Many class members have already experienced, or will soon experience, fraudulent credit and debit card purchases.

41. Also, many class members will incur out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, fees for replacement cards, and similar costs related to the Data Breach.

42. Class members also suffered a "loss of value" of their credit and debit card information when it was stolen by the hacker in the Data Breach. A robust market exists for stolen card information, which is sold on the dark web at specific identifiable prices. This market serves as a means to determine the loss of value to class members.

43. Class members also suffered "benefit of the bargain" damages. Class members overpaid for goods that should have been accompanied by adequate data security, but were not. Part of the price class members paid to Defendant was intended to be used to fund adequate data security. Class members did not get what they paid for.

44. Class members have spent and will continue to spend substantial amounts of time monitoring their credit and debit 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 disputing fraudulent charges, obtaining replacement cards, and resetting automatic payment links to their new cards. These efforts are burdensome and time-consuming.

45. Class members who experience actual fraud will also be 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. Those class members will also be harmed by the loss of use of and access to their account funds, and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they are permitted to obtain from their accounts. This includes missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations.

46. The stolen card information is a valuable commodity to identity thieves. Once cardholder information has been stolen, criminals often sell it on the cyber "black-market" or "dark web" indefinitely. Cyber criminals routinely post stolen credit and debit card information on anonymous websites, making the information widely available to a criminal underworld. There is an active and robust market for this information.

47. The risk of fraud will persist for years. Identity thieves often hold stolen data for months or years before using it. Also, the sale of stolen information on the dark web may take months or more to reach end-users, in part because the data may be sold in small batches as opposed to in bulk to a single buyer.

48. Thus, class members must vigilantly monitor their financial accounts for months or years to come.

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

49. Identity thieves can combine data stolen in the Data Breach with other information about class members gathered from underground sources, public sources, or even class members' social media accounts. Thieves can use the combined data to send highly targeted phishing emails to class members to obtain more sensitive information. Thieves can

also use the combined data to commit a variety of potential crimes including, *e.g.*, 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.

50. Defendant has acknowledged that class members face a significant risk of various type of identity theft stemming from the Data Breach. Defendant instructed all affected customers to: (i) review their credit and debit card statements carefully to identity fraudulent transactions; (ii) obtain a copy of their credit report to "look for any inaccuracies and/or accounts you don't recognize"; (iii) place a "fraud alert" on their 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 their credit file to prevent creditors from accessing the credit file without the consumer's consent.[11] Thus, Defendant concedes that class members face a risk of identity theft beyond just fraudulent credit and debit card transactions.

51. To protect against these broad-based types of fraud, Defendant offered one year of free credit monitoring and identity theft insurance to all customers whose card information was stolen in the Data Breach. This type of protection would not have been necessary if consumers' risk was limited to just fraudulent credit and debit card transactions.

V. CLASS ACTION ALLEGATIONS

52. Plaintiff brings this case as a class action pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of a Nationwide Class, a Pennsylvania Sub-Class, and a New Jersey Sub-Class (collectively, the "Classes"), defined as follows:

[11] https://www.wawa.com/alerts/data-security, Notice tab (last visited Dec. 21, 2019).

> Nationwide Class: All persons in the United States whose credit or debit card numbers were stolen in the data breach announced by Wawa on December 19, 2019.
>
> Pennsylvania Sub-Class: All residents of the state of Pennsylvania whose credit or debit card numbers were stolen in the data breach announced by Wawa on December 19, 2019.
>
> New Jersey Sub-Class: All residents of the state of New Jersey whose credit or debit card numbers were stolen in the data breach announced by Wawa on December 19, 2019.

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

54. Numerosity. The Classes are each so numerous that joinder of all members is impracticable. On information and belief, the Nationwide Class consists of millions of individuals, and the Pennsylvania Sub-Class and New Jersey Sub-Class each consist of tens of thousands or more individuals. These estimates are based on the fact that the Data Breach affected all or most of Defendant's 850 convenience store locations for a nine-month period.

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

a. Whether Defendant'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 Defendant owed a duty to class members to safeguard their payment card information;

c. Whether Defendant breached its duty to class members to safeguard their payment card information;

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

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

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

g. Whether Plaintiff and class members are entitled to injunctive relief.

56. Typicality. Plaintiff's claims are typical of the claims of all class members because Plaintiff, like other class members, suffered a theft of his cardholder information in the Data Breach.

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

58. Predominance. Defendant has engaged in a common course of conduct toward all class members. The common issues arising from Defendant's conduct predominate over any issues affecting just individual class members. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

59. 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 non-class 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 Defendant. 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.

60. Defendant 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, Pennsylvania Sub-Class, and New Jersey Sub-Class)

61. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

62. Defendant obtained class members' credit and debit card information in connection with class members' purchases at Defendant's stores.

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

64. Defendant owed a duty of care to Plaintiff and class members to provide data security consistent with the various requirements and rules discussed above.

65. Defendant's duty of care arose as a result of, among other things, the special relationship that existed between Defendant and its customers. Defendant 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. Defendant's breach announcement acknowledged that Defendant was in a "special relationship" with its customers for purposes of protecting their cardholder information.[12]

66. Also, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to use reasonable measures to protect confidential consumer data.

67. Defendant's duty to use reasonable care in protecting cardholder data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards and PCI DSS rules to protect cardholder information.

68. Defendant was subject to an "independent duty" untethered to any contract between class members and Defendant.

69. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect cardholder information. Defendant's negligent acts and omissions include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard cardholder information;

b. Failing to adequately monitor the security of Defendant's payment card processing network;

[12] https://www.wawa.com/alerts/data-security, Notice tab (last visited Dec. 21, 2019).

c. Allowing unauthorized access to class members' sensitive cardholder information;

d. Failing to detect in a timely manner that class members' cardholder information had been compromised; and

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

70. It was foreseeable to Defendant that a failure to use reasonable measures to protect cardholder information could result in injury to consumers. Further, actual and attempted breaches of data security were reasonably foreseeable to Defendant given the known frequency of payment card data breaches: (i) in the retail industry in general, and (ii) at Defendant's operations specifically.

71. Plaintiff and class members suffered various types of damages as alleged above.

72. Defendant's wrongful conduct was a proximate cause of class members' damages.

73. Plaintiff and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

74. Plaintiff and class members are also entitled to injunctive relief requiring Defendant to, *e.g.*,: (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 II

BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class, Pennsylvania Sub-Class, and New Jersey Sub-Class)

75. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

76. When Plaintiff and class members provided their card information to Defendant in exchange for Defendant's products, they entered into implied contracts with Defendant under which Defendant agreed to take reasonable steps to protect the card information.

77. Defendant solicited and invited class members to provide their card information as part of Defendant's regular business practices. Plaintiff and class members accepted Defendant's offers and provided their card information to Defendant.

78. When entering into the implied contracts, Plaintiff and class members reasonably believed and expected that Defendant's data security practices complied with relevant laws, regulations, and industry standards.

79. Defendant's implied promise to safeguard cardholder information is evidenced by, *e.g.*, the representations in Defendant's Privacy Policy set forth above.

80. Plaintiff and class members paid money to Defendant to purchase items at Defendant's convenience stores. Plaintiff and class members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

81. Plaintiff and class members would not have provided their card information to Defendant in the absence of Defendant's implied promise to keep the card information reasonably secure.

82. Plaintiff and class members fully performed their obligations under the implied contracts by paying money to Defendant.

83. Defendant breached its implied contracts with Plaintiff and class members by failing to implement reasonable data security measures.

84. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiff and class members sustained damages as alleged herein.

85. Plaintiff and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

86. Plaintiff and class members are also entitled to injunctive relief requiring Defendant to, *e.g.*,: (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 III

PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 Pa. Stat. §§ 201-1 to 201-9.2 (On Behalf of the Pennsylvania Sub-Class)

87. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

88. Plaintiff and Defendant are each a "person" as defined at 73 Pa. Stat. § 201-2(2).

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

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

91. Defendant engaged in "unfair methods of competition" or "unfair or deceptive acts or practices" as defined at 73 Pa. Stat. § 201-2(4) by 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 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)).

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

93. Defendant's unfair or deceptive acts and practices include but are not limited to: failing to implement and maintain reasonable data security measures to protect cardholder 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; and omitting and concealing the material fact that it did not have reasonable measures in place to safeguard cardholder data.

94. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security practices and ability to protect cardholder information.

95. Defendant intended to mislead consumers and induce them to rely on its misrepresentations and omissions.

96. Plaintiff and Pennsylvania Sub-Class members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered with reasonable diligence.

97. Had Defendant disclosed to consumers that its data security systems were not secure and, thus, were vulnerable to attack, class members would not have given their card data to Defendant.

98. Defendant acted intentionally, knowingly, and maliciously in violating the Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded consumers' rights.

99. Defendant'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.

100. As a direct and proximate result of Defendant's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and Pennsylvania Sub-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.

101. Plaintiff and Pennsylvania Sub-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, defied 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."

102. Plaintiff and Pennsylvania Sub-Class members also seek the injunctive relief as set forth above.

COUNT IV

NEW JERSEY CONSUMER FRAUD ACT
N.J. Stat. Ann. § 56:8-1, *et. seq*.
(On Behalf of the New Jersey Sub-Class)

103. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

104. Defendant sells "merchandise," which is defined by N.J. Stat. Ann. § 56:8-1(c) to include "goods" and "services."

105. Defendant engaged in unconscionable and deceptive acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the selling of merchandise, in violation of N.J. Stat. Ann. § 56:8-2, including but not limited to as follows:

a. Defendant misrepresented material facts to New Jersey Sub-Class members by representing that Defendant would maintain adequate data security practices and procedures to safeguard cardholder information from unauthorized disclosure, release, and theft;

b. Defendant misrepresented material facts to New Jersey Sub-Class members by representing that Defendant did and would comply with the requirements of relevant laws, regulations, and industry requirements regarding data privacy and security;

c. Defendant knowingly omitted the material fact of the inadequacy of its data security protections for cardholder information with the intent that consumers rely

on the omission, suppression, and concealment, regardless of whether consumers did in fact rely on the omission;

d. Defendant engaged in unconscionable and deceptive acts and practices with respect to the provision of its credit card payment function by failing to maintain the privacy and security of New Jersey Sub-Class members' cardholder information, in violation of duties imposed by applicable laws, regulations, industry standards, and Defendant's own Privacy Policy representations; and

e. Defendant engaged in unconscionable and deceptive acts and practices with respect to the sale of merchandise by failing to disclose the data breach to New Jersey Sub-Class members in a timely manner, in violation of N.J. Stat. Ann. § 56:8-163(a).

106. These unlawful and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous.

107. These acts caused substantial injury to consumers that the consumers could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

108. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard New Jersey Sub-Class members' cardholder information and that the risk of a data breach was unreasonably high. Defendant's actions in engaging in the above unfair practices and deceptive acts were knowing, willful, reckless, and/or negligent with respect to the rights of New Jersey Sub-Class members.

109. As a direct and proximate result of Defendant's unconscionable or deceptive acts and practices, New Jersey Sub-Class members suffered an "ascertainable loss of money or

property" under N.J. Stat. Ann. § 56:8-19, including the damages set forth above and the loss of their legally protected interest in the confidentiality of their payment card information.

110. New Jersey Sub-Class members seek relief under N.J. Stat. Ann. § 56:8-19, including but not limited to actual damages, treble damages, equitable relief, and attorneys' fees and costs.

RELIEF REQUESTED

Plaintiff, on behalf of all others similarly situated, requests that the Court enter judgment against Defendant including the following:

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

B. Appointing Plaintiff as a representative of each of the Classes and appointing Plaintiff's counsel as class counsel;

C. An award to Plaintiff and the Classes of compensatory, consequential, statutory, and treble damages as set forth above;

D. Ordering injunctive relief requiring Defendant to, *e.g.*,: (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;

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

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

G. Such other relief as the Court may allow.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury trial all issues so triable.

Dated: December 26, 2019

Respectfully submitted,

/s/ Sherrie R. Savett

Sherrie R. Savett (PA Bar No. 17646)
Shanon J. Carson (PA Bar No. 85957)
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
scarson@bm.net
jlambiras@bm.net

E. Michelle Drake
BERGER MONTAGUE, PC
43 SE Main Street, Suite 505
Minneapolis, MN 55414
Tel: (612) 594-5933
Fax: (612) 584-4470
emdrake@bm.net

Counsel for Plaintiff and the Classes

kal9491886