IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

ANDREA SILLS, JOSEPH DIVITA, and CORINNE M. MULLEN, on behalf of themselves, and all others similarly situated,

Plaintiffs,

v.

WAWA, INC.,
260 West Baltimore Pike
Wawa, PA 19063

Defendant.

_____/

Case No. _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs, Andrea Sills, Joseph DiVita and Corinne M. Mullen, by and through their counsel, assert the following claims in this class action against Defendant Wawa, Inc. ("Wawa" or "the Company"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

I. INTRODUCTION

1. Wawa is a trusted chain of convenience stores founded and operated in the Philadelphia region with market and market/fuel locations along the East Coast in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Washington, D.C. and Florida. On or about December 19, 2019, Wawa disclosed a breach of customer data that went undetected for nine months. Plaintiffs bring this class action on behalf of consumers against Wawa for the Company's failure to properly protect its customers' payment card data used at Wawa locations during the nine-month period including highly sensitive information such as credit or debit cardholder name, credit or debit card number, and expiration date ("Payment Card Data"). The Payment Card Data was stolen by hackers through the use of malware installed on Wawa's point-of-sale payment terminals, fuel

dispensers, and payment process servers from at least March 4, 2019 through December 12, 2019 (the "Wawa Data Breach" or "Data Breach").

2. Hackers accessed Wawa's inadequately protected point of sale systems and installed malware beginning on or about March 4, 2019 that infected potentially every Wawa in-store payment terminal and fuel dispenser in the United States.[1] With this malware, hackers stole the Payment Card Data of Wawa customers in locations throughout the United States where Wawa operates.

3. Many class members have experienced and will continue to experience the adverse impact of their data being stolen, including fraudulent credit or debit card purchases, as a foreseeable result of the Data Breach. Class members have and will suffer significant financial costs and injuries caused by Wawa's deficient data security measures, which include the theft of their personal and personal data, out-of-pocket costs to purchase protective measures such as credit monitoring services, credit freezes, and credit reports. They will also incur replacement card inconvenience and fees, as well as fees for additional items directly or indirectly related to the Data Breach.[2] Plaintiffs and class members have also lost their privacy.

4. Plaintiffs and class members have been exposed to a heightened and imminent risk of fraud and identity theft, including the imminent and impending injury flowing from potential fraud and identify theft posed by their credit card and personal information being placed in the hands of criminals and the risk of misuse via the sale of Plaintiffs and class members' information on the Internet black market. As such, class members must now and in the future (as

[1] Wawa, Wawa Notifies Customers of Data Security Incident, https://finance.yahoo.com/news/wawa-notifies-customers-data-security-210000289.html (Dec.19, 2019) (last accessed January 15, 2020).

[2] At least one New Jersey based bank closed approximately 2,000 debits cards because of the Wawa Data Breach as a precautionary measure. NJ bank closes debit accounts affected by Wawa breach (https://nj1015.com/nj-bank-closes-debit-accounts-affected-by-wawa-breach/) (last accessed January 15, 2020).

there is little ability to predict when the stolen data may be used) closely monitor their financial accounts to guard against fraud and maintenance of their privacy.

5. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose card information was stolen in the Data Breach. Plaintiffs seek 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.

Parties

6. Plaintiff Andrea Sills is a resident and citizen of New Castle County in the State of Delaware with an address of 2315 Ridgeway Road, Wilmington, DE 19805.

7. Plaintiff Joseph DiVita is a resident and citizen of Bucks County in the Commonwealth of Pennsylvania with an address of 5416 Lower Mountain Road, New Hope, PA 18938.

8. Plaintiff Corinne M. Mullen is a resident and citizen of Hudson County in the State of New Jersey with an address of 1201 Hudson Street, Apartment 230, Hoboken, NJ 07030.

9. Defendant Wawa, Inc. is a privately-held New Jersey corporation with its principal place of business in Wawa, Pennsylvania. It is a citizen of the Commonwealth of Pennsylvania.

10. Wawa is engaged in the business of developing and operating a system of 850 convenience stores throughout Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida, and Washington, D.C. Wawa offers gasoline at over 600 of these locations. According to *Forbes* magazine, Wawa ranked 25th on the list of largest private companies in 2019, with a reported total revenue of $12.1 billion.

11. Wawa is not a franchisor. It has total control over the manner in which its more than 850 locations operate, including those locations' computer software and electronic data transmission systems for point of sale reporting.

Jurisdiction and Venue

12. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d), because at least one Class member is of diverse citizenship from one defendant, there are more than 100 Class members, and the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs.

13. The Eastern District of Pennsylvania has personal jurisdiction over Defendant named in this action because Defendant is headquartered in Pennsylvania and conducts substantial business in Pennsylvania and this District through its headquarters, convenience stores, gas stations, and commercial website.

14. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered in this District and has caused harm to Plaintiffs and class members residing in this District.

II. FACTUAL ALLEGATIONS

The Data Breach is Disclosed

15. Approximately one month after it was warned by Visa, the nation's largest credit card network, of the threat to gas stations still using magnetic-stripe readers to accept card payments (instead of chip technology), Wawa discovered and then, nearly a week later, disclosed to the public the Data Breach. On December 19, 2019, Wawa posted on its corporate website "An Open Letter from Wawa CEO Chris Gheysens to Our Customers."

16. In what it termed its "official Notice," the Company addressed its customers advising that it had suffered a "data security incident" that compromised customers' sensitive Payment Card Data. The notice states:

> 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.[3]

17. The Notice further states the following about what information was involved:

> 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.

18. It is apparent from the little information that Wawa has published to date that it did not use the latest card encryption technology and thus, left its customers vulnerable to the hack.

19. Payment Card Data is valuable and frequently targeted by hackers. In a recent article, Business Insider noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers. At least 11 consumer companies reported data breaches in the last year. Many of them were caused by flaws in payment systems either online or in stores."[4]

---

[3] "Wawa Data Security – Updates & Customer Resources," WAWA (Dec. 19, 2019), https://www.wawa.com/alerts/data-security (last accessed January 15, 2020).

[4] Dennis Green & Mary Hanbury, "If you bought anything from these 11 companies in the last year, your data may have been stolen," BUSINESS INSIDER (Aug. 15, 2019), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1. (last accessed January 15, 2020).

20. Despite the known risk of a data breach and the widespread publicity and industry alerts regarding the other notable data breaches, and warning from the nation's top credit card network, Wawa failed to take reasonable steps to adequately protect its computer systems from being breached, and then failed to detect the Data Breach for several months. There is little doubt that Wawa could have prevented the breach and/or more timely discovered it by modernizing and upgrading their systems or establishing security protocols that more adequately monitored for malware.

21. Wawa is, and at all relevant times has been, aware that the Payment Card Data it maintains as a result of purchases made at its locations is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases.

22. Wawa recognizes the importance of adequately safeguarding its customers' sensitive Payment Card Data. On its website, Wawa states: "Protecting your privacy is important to Wawa." Its online Privacy Policy, last updated in June 2019—during the heart of the Wawa Data Breach - states that Wawa is "fully committed to data security." And despite Wawa recognizing the importance of its customers' privacy, and other than the on-line notice, Plaintiffs are unaware of any specific effort made to date to contact them or members of the Class about the breach.

23. Wawa is thus aware of the importance of safeguarding its customers' Payment Card Data from the foreseeable consequences that would occur if its data security systems were breached.

24. Financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants must take to ensure that consumers' valuable data is protected.

Wawa's Failure to Comply with Industry Standards for Data Security

25. Wawa failed to comply with industry standards for data security and actively mishandled the data entrusted to it by its customers.

26. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit Payment Card Data. These standards are known as the Payment Card Industry Data Security Standard ("PCI DSS"). PCI DSS is the industry standard governing the security of Payment Card Data, although it sets the minimum level of what must be done, not the maximum.

27. PCI DSS version 3.2.1, released in May 2018 and in effect at the time of the Data Breach, imposes 12 "high-level" mandates:[5]

28. Furthermore, PCI DSS 3.2.1 set forth detailed and comprehensive requirements that had to be followed to meet each of the 12 mandates.

29. Among other things, PCI DSS 3.2.1 requires Wawa to properly secure Payment Card Data; not store cardholder data beyond the time necessary to authorize a transaction; to timely upgrade its point-of-sale software; implement proper network segmentation; encrypt Payment Card Data at the point-of-sale; restrict access to Payment Card Data to those with a need to know; and establish a process to identify; and timely fix security vulnerabilities. Upon information and belief, Wawa failed to comply with each of these requirements.

---

[5] PCi Security Standards Council, *PCi DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1,* 9, July 2018, https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf (last accessed January 15, 2020).

Wawa Failed to Comply with Federal Trade Commission Requirements

30. According to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by §5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. §45.

31. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

32. The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

33. The FTC has issued orders against businesses that failed to employ reasonable measures to secure Payment Card Data. These orders provide further guidance to businesses with regard to their data security obligations.

34. In the years leading up to the Data Breach, and during the course of the breach itself, Wawa failed to follow the guidelines set forth by the FTC and actively mishandled the

management of its IT security. Wawa engaged in an unfair act or practice within the meaning of §5 of the FTC Act by failing to have reasonable data security measures in place.

III. PLAINTIFFS' TRANSACTIONS

35. Wawa failed to adhere to FTC standards to protect its customers' Payment Card Data and as a result, Plaintiffs and Class members have and will suffer various damage and loss.

36. During the period between March and December of 2019, Plaintiff Andrea Sills made approximately ten purchases inside a Wawa convenience location and purchased gas at a Wawa in the general Wilmington, DE area, but most purchases were made at 4030 Concord Pike, Talleyville, DE 19803 using credit cards issued to her by Capital One Visa and Citi Aadvantage MasterCard.

37. During the period between March and December of 2019, Plaintiff Joseph DiVita purchased gasoline at Wawa locations in Philadelphia, Pennsylvania and in New Jersey using his Wells Fargo debit card. Plaintiff DaVita made approximately 46 purchases using this debit card during this time, mostly for gasoline but occasionally within Wawa retail stores.

38. During the period between March and December of 2019, Plaintiff Corinne M. Mullen used her TD Bank Debit Card for a retail purchase at the Wawa on South River Street in Hackensack, New Jersey.

39. Plaintiffs would not have used their credit and/or debit cards to make purchases at Wawa had the Company told them that it lacked adequate computer systems and data security practices to safeguard customers' Payment Card Data from theft. Indeed, Plaintiffs would not have shopped at Wawa at all during the period of the Wawa Data Breach and, thus, they suffered actual injury and damages in paying money to Wawa for the purchase of products, including gasoline, from Wawa that they would not have paid had Wawa made such disclosure.

40. Plaintiffs also suffered actual injury in the form of damages to and diminution in the value of their Payment Card Data-a form of intangible property that Plaintiffs entrusted to Wawa for the purpose of purchasing its products and that was compromised in and as a result of the Wawa Data Breach.

41. Additionally, Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by their Payment Card Data being placed in the hands of criminals who stole and compromised Plaintiffs' payment card information.

42. Moreover, Plaintiffs have a continuing interest in ensuring that their private information, which remains in Wawa's possession, is protected and safeguarded from future breaches.

IV. CLASS ACTION ALLEGATIONS

43. Plaintiffs bring this action on behalf of themselves and as a class action, pursuant to the provisions of Rules 23(a), 23(b)(2), and 23(b)(3) of the Federal Rules of Civil Procedure, on behalf of the following class (the "Class"):

44. All persons in the United States who made a credit or debit card purchase at any affected Wawa location from March 4, 2019 to the present.

45. Excluded from the Class is Defendant and its subsidiaries and affiliates; all employees of Defendant; all persons who make a timely election to be excluded from the Class; government entities; and the judge to whom this case is assigned, including his/her immediate family and court staff.

46. Certification of Plaintiffs claims for Class-wide treatment is appropriate because all elements of Fed. R. Civ. P. 23(a), (b)(2)-(3) are satisfied. Plaintiffs can prove the elements of its

claims on a Class-wide basis using the same evidence as would be used to prove those elements in an individual action alleging the same claims.

47. **Numerosity**: All requirements of Fed. R. Civ. P. 23(a)(l) are satisfied. The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiffs are informed and believe that there are thousands of members of the Class, the precise number of Class members is unknown to Plaintiffs. Plaintiffs believe that the identity of Class members is known or knowable by Wawa. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

48. **Commonality and Predominance**: All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

a. whether Defendant engaged in the active misfeasance and misconduct alleged herein;

b. whether Wawa owed a duty to Plaintiffs and members of the Class to act reasonably to protect Payment Card Data;

c. whether Wawa failed to provide adequate security to protect Payment Card Data;

d. whether Wawa negligently, or otherwise improperly, allowed third parties to access Payment Card Data;

e. whether Plaintiffs and members of the Class were injured and suffered damages and ascertainable losses;

f. whether Wawa's failure to provide adequate security proximately caused Plaintiffs' and Class members' injuries;

g. whether Plaintiffs and members of the Class are entitled to damages and, if so, the measure of such damages; and

h. whether Plaintiffs and members of the Class are entitled to declaratory and injunctive relief.

49. **Typicality**: All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiffs are a member of the Class, having used their payment cards at affected Wawa locations and had their Payment Card Data compromised in the Data Breach. Plaintiffs' claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through Defendant's conduct.

50. **Adequacy of Representation**: All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiffs are adequate Class representatives because they are a member of the Class and their interests do not conflict with the interests of the other members of the Class that they seek to represent. Plaintiffs are committed to pursuing this matter for the Class with the Class's collective best interests in mind. Plaintiffs have retained counsel competent and experienced in complex class action litigation of this type and Plaintiffs intend to prosecute this action vigorously. Plaintiffs, and their counsel, will fairly and adequately protect the Class's interests.

51. **Predominance and Superiority**: All requirements of Ped. R. Civ. P. 23(b)(3) are satisfied. As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in Plaintiffs' individual cases will also resolve them for the Class's claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered

in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

52. **Cohesiveness**: All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Defendant has acted, or refused to act, on grounds generally applicable to the Class making final declaratory or injunctive relief appropriate.

V. CHOICE OF LAW

53. Wawa's acts and omissions discussed herein were orchestrated and implemented at its corporate headquarters in Pennsylvania and the tortious and deceptive acts complained of occurred in, and radiated from, Pennsylvania.

54. The key wrongdoing at issue in this litigation (Wawa's failure to employ adequate data security measures) emanated from Wawa's headquarters in Pennsylvania.

55. Upon information and belief, Wawa's point-of-sale system and IT personnel operate out of and are located at Wawa's headquarters in Pennsylvania.

56. Pennsylvania, which seeks to protect the rights and interests of Pennsylvania and other U.S. citizens against a company doing business in Pennsylvania, has a greater interest in the

claims of Plaintiff and the Class members than any other state and is most intimately concerned with the outcome of this litigation.

57. Application of Pennsylvania law to a nationwide Class with respect to Plaintiffs and the Class members' claims is neither arbitrary nor fundamentally unfair because Pennsylvania has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiff and the nationwide Class.

VI. CAUSES OF ACTION

COUNT 1
Negligence

On behalf of the Plaintiffs and the Class

58. Plaintiffs incorporate by reference all preceding allegations, as though fully set forth herein.

59. Wawa owed and continues to owe a duty to Plaintiffs and the Class to use reasonable care in safeguarding Payment Card Data and to discover any breach in a timely manner, so that compromised financial accounts and credit cards can be frozen and/or closed quickly in order to avoid fraudulent transactions. This duty arises from several sources, including, but not limited to, the sources described below, and is independent of any duty Wawa owed as a result of its contractual obligations.

60. Wawa has a common law duty to prevent the foreseeable risk of harm to others, including Plaintiffs and the Class. It was certainly foreseeable to Wawa that injury would result from a failure to use reasonable measures to protect Payment Card Data and to detect breaches in a timely manner. It was also foreseeable that, if reasonable security measures were not taken, hackers would steal Payment Card Data belonging to millions of Wawa's customers; thieves would

use Payment Card Data to make large numbers of fraudulent transactions; and that the resulting financial losses would be immense.

61. Wawa assumed the duty to use reasonable security measures as a result of its conduct.

62. In addition to its general duty to exercise reasonable care, Wawa also had a duty of care as a result of the special relationship that existed between Wawa and Plaintiffs and members of the Class. The special relationship arose because customers entrusted Wawa with their Payment Card Data. Only Wawa was in a position to ensure that its systems were sufficient to protect against the harm to its customers from a data breach.

63. Wawa's duty to use reasonable data security measures also arose under §5 of the FTC Act, which prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Payment Card Data by businesses such as Wawa. The FTC publications and data security breach orders described above further form the basis of Wawa's duty. In addition, individual states have enacted statutes based upon the FTC Act that also create a duty on the part of Wawa.

64. Wawa's duty to use reasonable care in protecting Payment Card Data arose not only as a result of the common law and the statutes described above, but also because it was bound by, and had committed to comply with, industry standards, specifically including PCI DSS.

65. Wawa breached its common law, statutory, and other duties and thus, was negligent by failing to use reasonable measures to protect Plaintiffs' Payment Card Data from the hackers who perpetrated the data breach and by failing to discover the breach timely. Upon information and belief, the specific negligent acts and omissions committed by Wawa include, but are not limited to, some, or all, of the following:

a. failure to delete cardholder information after the time period necessary to authorize the transaction;

b. failure to employ systems to protect against malware;

c. failure to comply with industry standards for software and point-of-sale security;

d. failure to track and monitor access to its network and cardholder data;

e. failure to limit access to those with a valid purpose;

f. failure to adequately staff and fund its data security operation;

g. failure to use due care in hiring, promoting, and supervising those responsible for its data security operations; and

h. failure to recognize that hackers were stealing Payment Card Data from its network while the data breach was taking place.

66. In connection with the conduct described above, Wawa acted wantonly, recklessly, and with complete disregard for the consequences.

67. As a direct and proximate result of Wawa's negligence, Plaintiffs and members of the Class have and will suffer actual losses and damages as described above.

COUNT II
Negligence Per Se

On behalf of the Plaintiffs and the Class

68. Plaintiffs incorporate by reference all preceding allegations, as though fully set forth herein.

69. Section 5 of the FTC Act prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as

Wawa, of failing to use reasonable measures to protect Payment Card Data. The FTC publications and orders described above also form part of the basis of Wawa's duty.

70. Wawa violated §5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Payment Card Data and not complying with applicable industry standards, including PCI DSS, as described in detail herein. Wawa's conduct was particularly unreasonable given the nature and amount of Payment Card Data it obtained and stored and the foreseeable consequences of a data breach at one of the country's largest private companies, including, specifically, the immense damages that would result to consumers and financial institutions.

71. Wawa's violation of §5 of the FTC Act (and similar state statutes) constitutes negligence per se.

72. Plaintiffs and members of the Class are within the class of persons that §5 of the FTC Act (and similar state statutes) was intended to protect.

73. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the Class.

74. As a direct and proximate result of Wawa's negligence, Plaintiffs and members of the Class have and will suffer actual losses and damages as described above.

COUNT III
Unjust Enrichment

On behalf of the Plaintiffs and the Class

75. Plaintiffs incorporate by reference all preceding allegations, as though fully set forth herein.

76. Plaintiffs and Class members conferred a monetary benefit on Wawa. Specifically, they purchased goods and services from Wawa and provided Wawa with their payment information. In exchange, Plaintiffs and Class members should have received from Wawa the goods and services that were the subject of the transaction and should have been entitled to have Wawa protect their Payment Card Data with adequate data security.

77. Wawa knew that Plaintiffs and Class members conferred a benefit on Wawa and accepted and has accepted or retained that benefit. Wawa profited from the purchases and used the Payment Card Data of Plaintiffs and Class members for business purposes.

78. Wawa failed to secure the Payment Card Data of Plaintiffs and Class members and, therefore, did not provide full compensation for the benefit the Plaintiffs and Class members provided.

79. Wawa acquired the Payment Card Data through inequitable means it failed to disclose the inadequate security practices previously alleged.

80. If Plaintiffs and Class members knew that Wawa would not secure their Payment Card Data using adequate security, they would not have made purchases at Wawa' s convenience stores.

81. Plaintiffs and Class members have no adequate remedy at law.

82. Under the circumstances, it would be unjust for Wawa to be permitted to retain any of the benefits that Plaintiffs and Class members conferred on it.

83. Wawa should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that it unjustly received from them. In the alternative, Wawa should be compelled to refund the amounts that Plaintiffs and Class. members overpaid.

COUNT IV
Violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Cons. Stat. §§ 201-2 & 201-3, et seq.

On behalf of the Plaintiffs and the Class

84. Plaintiffs incorporate by reference all preceding allegations, as though fully set forth herein.

85. Wawa is a "person", as defined by 73 Pa. Cons. Stat. § 201-2(2).

86. Plaintiffs and Class Members purchased goods and services in "trade" and "commerce," as defined by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

87. Wawa engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including:

a. Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

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

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

88. Wawa's unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' Personal data , which was a direct and proximate cause of the Data Breach;

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

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring their vendors and business associates maintained reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and 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 Plaintiffs' and Class Members' Personal data or ensure its vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal data, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

90. Wawa intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

91. Had Wawa disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Wawa would have been forced to use vendors and business associates with reasonable data security measures and comply with the law. Instead, Wawa received, maintained, and compiled Plaintiffs' and Class Members' Personal data as part of the services it provided without advising Plaintiffs and Class Members that its data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Class Members' Personal Information. Accordingly, Plaintiffs and Class Members acted reasonably in relying on Wawa's misrepresentations and omissions, the truth of which they could not have discovered.

92. Wawa acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiffs' and Class Members' rights.

93. As a direct and proximate result of Wawa's unfair methods of competition and unfair or deceptive acts or practices and Plaintiffs' and Class Members' reliance on them, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money

or property, and monetary and non-monetary damages; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal data ; and an increased, imminent risk of fraud and identity theft.

94. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100 (whichever is greater), treble damages, restitution, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

COUNT V
Violation of the New Jersey Consumer Fraud Act, N.J.S.A. § 56:8-1, et seq.

On behalf of the Plaintiffs and the Class

95. Plaintiffs incorporate by reference all preceding allegations, as though fully set forth herein.

96. The New Jersey Consumer Fraud Act (the "NJCFA"), N.J.S.A. § 56:8-1, et seq., 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, in connection with the sale or advertisement of any merchandise. The NJCFA applies whether or not any person has in fact been misled, deceived or damaged thereby. N.J.S.A.§ 56:8-2.

97. Plaintiffs, Wawa, and Class Members are "persons" within the meaning of N.J.S.A. § 56:8-1(d).

98. Wawa sells "merchandise," as defined by N.J.S.A. § 56:8-1, by offering convenience store goods and services to the public.

99. Wawa, operating in New Jersey, engaged in unconscionable and deceptive acts

and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of convenience store goods and services in violation of N.J.S.A. § 56:8-2, including but not limited to the following:

a. Misrepresenting material facts, pertaining to the sale of convenience store goods and services, to Plaintiffs and Class Members by representing that it would maintain adequate data security practices and procedures to safeguard Plaintiffs' and Class Members' personal data from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts, pertaining to the sale of convenience store goods and services, to Plaintiffs and Class Members by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiffs' and Class Members' personal data ;

c. Knowingly omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiffs' and Class Members' personal data with the intent that Plaintiffs and Class Members rely on the omission, suppression, and concealment;

d. Engaging in unconscionable and deceptive acts and practices with respect to the sale of convenience store goods and services by failing to adequately monitor and audit the data security systems of its vendors and business associates and failing to maintain the privacy and security of Plaintiffs and Class Members in violation of duties imposed by and public policies reflected in the FTC Act;

e. Engaging in unconscionable and deceptive acts and practices by failing to disclose the Data Breach to Plaintiffs and Class Members in a timely and accurate manner in violation of N.J.S.A. § 56:8-163;

f. Advertising Wawa's goods and services with the intent not to sell it as advertised – i.e., with worse data security than advertised; and

g. Representing on its website that it is "is fully committed to data security" when, in fact, Wawa failed to safeguard customers' information by relying on deficient data security protection.

100. The above unlawful and deceptive acts and practices by Wawa were immoral, unethical, oppressive, and unscrupulous. 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.

101. Wawa knew or should have known that its data security practices were inadequate to safeguard Plaintiffs' and Class Members' personal data and that the risk of a data breach was highly likely. Wawa's actions in engaging in the above-listed unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class Members.

102. Plaintiffs and Class Members reasonably expected that Wawa would protect their Personal data and reasonably expected that Wawa would provide truthful statements on its website and privacy policies, and that it would be safe to provide Wawa with their information. These representations and affirmations of fact made by Wawa, and the facts it concealed or failed to disclose, are material facts that were likely to deceive reasonable consumers, and that reasonable consumers would, and did, rely upon in deciding whether or not to provide their information to

Wawa. Wawa, moreover, intended for consumers, including Plaintiffs and Class Members, to rely on these material facts.

103. As a direct and proximate result of Wawa's unconscionable and deceptive acts and practices, Plaintiffs and Class Members suffered an ascertainable loss in moneys or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their personal data .

104. Plaintiffs and Class Members seek relief under N.J.S.A. § 56:8-19, including but not limited to, injunctive relief, other equitable relief, actual damages, treble damages, and attorneys' fees and costs.

COUNT VI
Violation of the New Jersey Customer Security Breach Disclosure Act, N.J.S.A. §§ 56:8163, et seq.

On behalf of the Plaintiffs and the Class

105. Plaintiffs incorporate by reference all preceding allegations, as though fully set forth herein.

106. Wawa is incorporated under the laws of the State of New Jersey and regularly conducts business in New Jersey under N.J.S.A. § 56:8-163(a).

107. Plaintiffs' and Class Members' personal data includes personal information covered under N.J.S.A. §§ 56:8-163, et seq.

108. Under N.J.S.A. § 56:8-163(a), "[a]ny business that conducts business in New Jersey. . . shall disclose any breach of security of [] 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."

109. Because Wawa discovered a breach of its security system involving the Personal

data of Plaintiffs and Class Members, in which such personal data was, or is reasonably believed to have been, acquired by an unauthorized person, and the personal data was not secured, Wawa had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated under N.J.S.A. §§ 56:8-163, et seq.

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

111. As a direct and proximate result of Wawa's violations of N.J.S.A. § 56:8-163(a), Plaintiffs and Class Members suffered the damages described above.

112. Plaintiffs and Class Members seek relief under N.J.S.A. § 56:8-19, including treble damages, attorneys' fees and costs, and injunctive relief.

COUNT VII
Declaratory and Injunctive Relief

On behalf of the Plaintiffs and the Class

113. Plaintiffs incorporate by reference all preceding allegations, as though fully set forth herein.

114. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described herein.

115. An actual controversy has arisen in the wake of Wawa's data breach regarding its common law and other duties to reasonably safeguard Payment Card Data. Plaintiffs allege that Wawa's data security measures were inadequate and remain inadequate.

116. Wawa still possesses Payment Card Data pertaining to Plaintiffs and Class members.

117. Wawa has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its POS systems and fueling stations.

118. Accordingly, Wawa has not satisfied its legal duties to Plaintiffs and Class members. In fact, now that Wawa's lax approach towards data security has become public, the Payment Card Data in its possession is more vulnerable than previously.

119. Actual harm has arisen in the wake of the Wawa Data Breach regarding Wawa's duties of care to provide data security measures to Plaintiffs and Class members.

120. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Wawa continues to owe a legal duty to secure its customers' personal and financial information-specifically including information pertaining to credit and debit cards used by Wawa's customers-and to notify financial institutions of a data breach under the common law, §5 of the FTC Act, PCI DSS standards, its commitments, and various state statutes;

b. Wawa continues to breach this legal duty by failing to employ reasonable measures to secure its customers' personal and personal data; and

c. Wawa's ongoing breaches of its legal duty continue to cause Plaintiff harm.

121. The Court also should issue corresponding injunctive relief requiring Wawa to employ adequate security protocols, consistent with industry standards, to protect its Payment Card Data. Specifically, this injunction should, among other things, direct Wawa to:

a. utilize industry standard encryption to encrypt the transmission of cardholder data at the point-of-sale and at all other times;

b. implement encryption keys in accordance with industry standards;

c. implement EMV technology;

d. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

e. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

f. regularly test its systems for security vulnerabilities, consistent with industry standards;

g. comply with all PCI DSS standards pertaining to the security of its customers' personal and confidential information; and

h. install all upgrades recommended by manufacturers of security software and firewalls used by Wawa.

122. If an injunction is not issued, Plaintiffs will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Wawa. The risk of another such breach is real, immediate, and substantial. If another breach at Wawa occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiffs and the Class for out of pocket damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiffs and the Class, which include monetary damages that are not legally quantifiable or provable.

123. The hardship to Plaintiffs and the Class, if an injunction is not issued, exceeds the hardship to Wawa, if an injunction is issued. Among other things, if another massive data breach occurs at Wawa, Plaintiffs and members of the Class will likely incur hundreds of millions of

dollars in damage. On the other hand, the cost to Wawa of complying with an injunction by employing reasonable data security measures is relatively minimal and Wawa has a pre-existing legal obligation to employ such measures.

124. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Wawa, thus eliminating the injuries that would result to Plaintiffs, the Class, and the millions of consumers whose confidential information would be compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class, respectfully requests that the Court:

A. Certify the Class and appoint Plaintiffs and Plaintiffs' counsel to represent the Class;

B. Enter a monetary judgment in favor of Plaintiffs and members of the Class to compensate them for the injuries suffered, together with pre-judgment and post-judgment interest, treble damages, and penalties where appropriate;

C. Enter a declaratory judgment in favor of Plaintiffs and the Class, as described above;

D. Grant Plaintiffs the injunctive relief requested;

E. Award Plaintiffs and the Class reasonable attorneys' fees and costs of suit, as allowed by law; and

F. Award such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury.

Dated: January 15, 2020

Respectfully submitted,

WEIR & PARTNERS LLP

By: _____

Steven E. Angstreich, Esquire (#3739)
Brett A. Datto, Esquire (59493)
Amy R. Brandt, Esquire (#65739)
The Widener Building, Suite 500
1339 Chestnut Street
Philadelphia, PA 19107
(215) 665-8181
(215) 665-8464 Fax
sangstreich@weirpartners.com
brett.datto@weirpartners.com
abrandt@weirpartners.com

GEORGE GESTEN MCDONALD, PLLC
David J. George, Esquire (FL # 898570)
Ryan D. Gesten, Esquire (FL #240760)
Matthew R. Chiapperini, Esquire (FL #111417)
9897 Lake Worth Road, Suite #302
Lake Worth, FL 33467
(561) 232-6002
(888) 421-4173 Fax
dgeorge@4-justice.com
RGesten@4-Justice.com
MChiapperini@4-Justice.com

GEORGE GESTEN MCDONALD, PLLC
Lori G. Feldman, Esquire (NY #2389070)
102 Half Moon Bay Drive
Croton On Hudson, NY 10502
(917) 983-9321
(888) 421-4173 Fax
LFFeldman@4-Justice.com

MORRISON & ASSOCIATES
Mark Morrison, Esquire (CA #152561)
113 Cherry Street, Suite 34835
Seattle, WA 98104
(360) 440-0734
Mark@mpaclassactions.com