$400

GEKP

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

ROB ROESSLE, individually and on behalf of all others who are similarly situated, Plaintiff, v. WAWA, INC., Defendant.	Civil Action No. 19 6161 **COMPLAINT - CLASS ACTION** **Jury Trial Demanded**

Plaintiff Rob Roessle by and through his undersigned counsel, brings this Class Action Complaint against Wawa Incorporated, on behalf of himself and all others similarly situated, and alleges, upon personal knowledge as to his own actions, upon his counsel's investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Wawa, Inc. (referred herein as "Wawa" or "Defendant") for its failure to secure and safeguard its customers' names, credit card and debit card numbers, credit card and debit card expiration dates, other payment data ("PCD"), and other personally identifiable information ("PII") which Wawa collected at the time Plaintiff made a purchase at a Wawa location (collectively, "Customer Data"), and for failing to provide timely, accurate, and adequate notice to Plaintiff and other class members that their Customer Data had been stolen, and precisely which types of information were stolen.

2. On December 19, 2019 at 4:00 PM EST Wawa announced that customers at all 850 Wawa locations had their Customer Data stolen starting at least on March 4, 2019 through December 10, 2019 (the "Data Breach"). Wawa, through its failure to maintain adequate data

safety protocols, allowed hackers to access Customer Data for nearly ten months before Wawa's information security team discovered the Data Breach on December 10, 2019. According to Wawa, it fully contained the Data Breach on December 12, 2019. Wawa then waited nearly a week before notifying customers that there had been a massive data breach.

3. On December 21, 2019, the Philadelphia Enquirer reported that Wawa's investigation was still on-going and that Wawa had summoned the assistance of the Federal Bureau of Investigation ("FBI").[1]

4. Wawa has yet to disclose the approximate number of customers whose Customer Data was appropriated by unauthorized third parties during the nearly ten-month long Data Breach period. To approximate the potential scale of this Data Breach: according to Wawa, the company serves approximately 400,000,000 customers per year which means nearly 1/3 of a billion customers during the Data Breach period.[2]

5. Hackers installed malware designed to steal credit card and debit card data on Wawa's point-of-sale ("POS") systems. Wawa has yet to indicate how the hackers gained access to Wawa's POS systems, or how the hackers were able to continue their hack undetected for such an extended period of time.

6. The Customer Data stolen as a result of the Data Breach includes cardholder names, credit and/or debit card information, expiration dates, and other possible PCD.

7. Wawa could have prevented this Data Breach. There have been prevalent data breaches at other retail establishments in the last few years as the result of malware installed on POS systems. While many retailers, banks, and other brick-and-mortar establishments responded

[1] Philadelphia Inquirer, *Wawa Data Breach*, https://www.inquirer.com/news/wawa-data-breach-credit-debit-card-fbi-investigation-20191221.html

[2] CSP Daily News, *Wawa Profile*, https://www cspdailynews com/top-202-convenience-stores-2016/wawa

to those recent breaches by modernizing their technology, upgrading their systems, or establishing security protocols that monitored for malware that helps makes transactions more secure, Wawa failed to adequately do so.

8. Wawa disregarded the rights of Plaintiff and Class members by failing to take adequate steps to prevent and stop the breach from ever happening, and failing to disclose to its customers the material fact that Wawa lacks adequate computer systems and security practices to safeguard customers' Customer Data.

9. On information and belief, the Customer Data of Plaintiff and Class members was improperly handled and stored and was not kept in accordance with applicable and required cyber-security protocols, policies and procedures. As a result, the Customer Data of Plaintiff and Class members was compromised and stolen. Moreover, as this same information remains stored in Wawa's computer system, which Wawa has shown an inability to safeguard, Plaintiff and Class members have an interest in ensuring that their information is safe, and that they should be entitled to seek injunctive and other relief, including independent oversight of Wawa's security systems.

PARTIES

10. Plaintiff Rob Roessle is a resident of the commonwealth of Virginia. Mr. Roessle regularly shops at Wawa locations in Virginia, specifically the Wawa location in Mechanicsville, Virginia. After Mr. Roessle shopped at Wawa during the Data Breach period, Mr. Roessle was contacted in November 2019 by his bank (BB&T) about his debit card being compromised. According to BB&T, someone was trying to use the card in order to make a purchase at a towing yard in the State of New York; the attempt was unsuccessful, as it was blocked by Mr. Roessle's bank. To the best of his knowledge, the misuse of Mr. Roessle's debit card was caused by the Data Breach. To the best of his knowledge, Mr. Roessle's debit card and BB&T account were not involved in any other data breaches other than the Wawa Data Breach.

11. Defendant Wawa, Incorporated is a New Jersey corporation and maintains its headquarters in Wawa, Pennsylvania.

12. Wawa operates a chain of convenience stores, and sells food, beverages, gasoline, and other convenience items. As of December 23, 2019, there are more than 850 Wawa locations in the United States with stores in New Jersey, Pennsylvania, Delaware, Maryland, Virginia, Washington D.C., and Florida.[3]

JURISDICTION AND VENUE

13. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. 1332(d). The aggregated claims of the individual class members exceed $5,000,000, exclusive of costs and interest, there are over 100 class members, and this is a class action in which one plaintiff is from a different state from the Defendant.

14. This Court has jurisdiction over Defendant Wawa because Wawa is headquartered in the District and operates locations serving the public in this District. Wawa also advertises in a variety of media throughout several states, including in Pennsylvania, as well as this District. Through its business operations in this District, Wawa intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

15. Venue is proper in this District pursuant to 28 U.S.C. 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District, Wawa is headquartered in this District, Wawa operates locations in this District, and Wawa has caused harm to Class members residing in this District.

[3] Wawa Press Release (Dec. 19, 2019), https://www prnewswire com/news-releases/wawa-notifies-customers-of-data-security-incident-300977948 html

FACTUAL BACKGROUND

A. Wawa and Its Customer Data Collection Practices

16. Wawa gains its revenue from store operations. When customers make purchases at Wawa locations, they commonly pay using credit or debit cards. According to Wawa's privacy policy, Wawa collects PII and PCD related to that card, including the name of the cardholder, the number on the card itself, and the expiration date.[4] Wawa stores this information in its point-of-sale system at the moment the card is swiped at the time of purchase.

B. Stolen Customer Data Is Valuable to Hackers and Thieves

17. PII and PCD are categories of information frequently targeted by hackers. Numerous hacks targeting customers' information have put Wawa on notice that identity thieves target PII and that hackers will go to great lengths to attain PII.

18. Over the past decade, recent large-scale breaches have targeted PII held by Wendy's, Marriott, Equifax, Yahoo, Anthem, Premera, Target, and many other companies. Indeed, Wawa itself suffered a data breach in 2013, when Wawa customers had their credit card numbers stolen from a Wawa location in New Jersey - this, on its own, should have put Wawa on notice as to the necessity to adequately protect Customer Data.

19. According to Experian, 14.2 million Americans had their credit card numbers stolen in 2017 an 88% increase in the amount of credit cards numbers stolen in the U.S. from 2016.[5]

20. Regardless of the new prevalence of data breaches and fact that data breaches have become common at retail locations, Wawa has maintained an inadequate system to protect the PII and PCD of Plaintiff and Class members. Wawa had a duty pursuant to common law, acceptable

[4] Wawa, *Data Security and Privacy Policy*, https //www wawa.com/alerts/data-security.

[5] Experian, *Identity Theft Statistics*, https://www.experian.com/blogs/ask-experian/identity-theft-statistics/

industry standards, credit/debit card network regulations, and representations made in its own privacy policy to keep Customer Data secure and to protect it from unauthorized access.

21. Plaintiff would not have provided the same types and amounts of PII and PCD to Wawa had he known that Wawa fails to take reasonable and necessary precautions to secure such information.

22. As a result, Wawa failed to maintain reasonable and adequate data security, thereby allowing the Data Breach affecting potentially 1/3 of a billion customer purchases on the east coast of the United States.

C. Wawa Failed to Maintain Proper PCI Data Security Standards

23. Merchants who agree to allow credit card and debit cards to be used at their locations must consent to minimal industry standards called the Payment Card Industry Data Security Standards ("PCI DSS").[6] This system sets the very minimum standards of conduct that merchants should be upholding.

24. The PCI DSS requires that merchants protect all data from malware and to regularly check for the existence of malware on system servers. Wawa failed to do so -- Wawa failed to meet the minimum standards set forth by PCI DSS.

D. Wawa Failed to Comply with the FTC's Requirements

25. In 2007, the Federal Trade Commission released a set of industry standards related to data security and the data security practices of businesses called *Protecting Personal Information: A Guide for Businesses* (the "guide").[7]

---

[6] PCI Security Standards Council, *PCI Data Sec. Standards (PCI DSS)*, https://www pcisecuritystandards org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1577046042482.

[7] FTC, *Protecting Personal Information*, https //www ftc gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

26. In 2011, the guide was updated to include fundamental data security principles for businesses. In addition to the necessity to protect consumer data, the guide established that:

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

27. Wawa failed to adequately address any of these requirements enumerated in the guide.

28. In 2015, the FTC supplemented the guide once more with a publication called *Start with Security.*[8] This supplement added further requirements for businesses that maintain Customer Data on their networks:

- Businesses should not keep PII and PCD stored on their networks for any period longer than what is needed for authorization;

[8] FTC, *Start with Security*, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

- Businesses should use industry-tested methods for data security; and,
- Businesses should be continuously monitoring for suspicious activity on their network.

29. Again, Wawa failed to adequately address any of these requirements enumerated in the supplemented guide.

30. The failure to follow the guide and the supplemental guide, as well as the failure to employ appropriate protocols and practices to protect against unauthorized access to confidential consumer data, constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. Sect. 45.

E. The Data Breach

31. In early March of 2019, hackers penetrated Wawa's computer systems.[9]

32. By April 22, 2019, the hackers breached and accessed Wawa's Point-of-Sale systems at all 850+ Wawa locations dispersed throughout the east coast of the United States.[10] With this access, the hackers were able to install malicious malware on the Point-of-Sale systems at each of Wawa's stores.[11]

33. On December 10, 2019, nearly ten months after the hackers initially gained access to Wawa's systems, Wawa finally discovered the presence of the hackers' malware stealing PII and PCD from Wawa's Point-of-Sale systems.[12]

[9] https://www.wawa.com/alerts/data-security

[10] *Id*

[11] *Id*

[12] *Id*

34. On December 12, 2019, two days after discovering the presence of the hackers' malware, Wawa finally isolated the threat and stopped the theft of PII and PCD from Wawa's Point-of-Sale systems.[13]

35. On December 19, 2019, nearly a full week after isolating the threat, Wawa finally announced that the Data Breach had taken place.[14] According to Wawa's press release disseminated by CEO Chris Gheysens:

> "I want to reassure you that you will not be responsible for any fraudulent charges on your payment cards related to this incident, as described in the detailed information below. Please review this entire letter carefully to learn about the resources Wawa is providing and the steps you should take now to protect your information.
>
> I apologize deeply to all of you, our friends and neighbors, for this incident. You are my top priority and are critically important to all of the nearly 37,000 associates at Wawa. We take this special relationship with you and the protection of your information very seriously. I can assure you that throughout this process, everyone at Wawa has followed our longstanding values and has worked quickly and diligently to address this issue and inform our customers as quickly as possible."

36. However, according to the Plaintiff, he has yet to have been contacted by Wawa as of December 27, 2019. The December 19, 2019 press release was merely an attempt to pacify concerned customers who were rightfully alarmed about the nature of the confidential Customer Data which was stolen directly from Wawa's poorly protected Point-of-Sale systems.

37. Wawa's press release contained numerous material omissions, including:

(a) Wawa failed to disclose the credit card and debit card numbers which were compromised as a result of the Data Breach;

(b) Wawa failed to disclose how many customers were affected by the Data Breach.

---

[13] *Id*

[14] *Id*

38. In the press release, Wawa acknowledged that Plaintiff and other Wawa customers face significant identity theft risks. Specifically, Wawa instructed all customers who made credit card or debit card purchases during the Data Breach period to take the following mitigating steps: (1) review credit card and debit card statements to identify questionable or fraudulent transactions, (2) check their credit scores and credit reports to ascertain whether any inconsistencies exist, (3) activate fraud tracking alerts if their credit monitoring agency contains such systems, and (4) activate a "security freeze" on all credit files to prevent any sort of deleterious effects of identity theft from affecting their credit history or credit scores.

39. Aside from this information, Wawa remains opaque, as much of what is known about the Data Breach is being made public through media outlets. For example, the Philadelphia Inquirer reported Wawa has contacted private investigators as well as the FBI to assist in their on-going investigation related to the Data Breach; this is a good example of information that Wawa should have told to the public.

F. The Data Breach Caused Harm and Will Result in Additional Fraud

40. The potential effects of Wawa's continued failure to keep Plaintiff and Class members' data safe are dire.

41. According to the FTC, identity theft is "a fraud committed or attempted using the identifying information of another person without authority."[15] The FTC defines identifying information as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[16]

[15] 17 C.F.R. Sect. 248.201 (2013).

[16] *Id*

42. The hackers are already likely using the Customer Data they have stolen from Wawa to attempt to commit fraud and identity theft, as has occurred to the Plaintiff as alleged herein.

43. PII and PCD are invaluable assets to hackers once the information has been compromised. Statistics estimate that tens of millions of Americans have their identities stolen each year because of how valuable this information can be.[17] This information gives hackers the ability to try to apply for new credit or debit cards, attempt to make purchases online, attempt to procure medical care on the hacked person's health insurance, attempt to gain access to the hacked person's bank accounts, and, if they have the right information, even collect the hacked person's tax refund from the Internal Revenue Service.

44. As a result of Wawa's failures, Plaintiff and Class members now face years of concern, frustration and emotional distress about their financial and personal records being stolen. The Plaintiff and Class are incurring, and will continue to incur, damages in addition to any fraudulent credit and debit card charges and the resulting loss of use of their credit and access to funds – regardless if these charges are subsequently reimbursed by the credit card companies.

G. Plaintiffs and Class Members Suffered Damages

45. The Data Breach was a direct and proximate cause of Wawa's failure to properly safeguard and protect the Plaintiff and Class members' Customer Data from unauthorized access, use, and disclosure, as required by state and federal regulations, industry standard, and the common law, including Wawa's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

[17] Experian, *Identity Theft Statistics*, https://www.experian.com/blogs/ask-experian/identity-theft-statistics/

46. Plaintiff and Class members' PII was not properly protected by Wawa. Wawa did not obtain Plaintiff and Class members' consent to disclose their PI or PCD to any other person as required by law and by industry standards.

47. Specifically, Wawa breached its duties, obligations and promises to the Plaintiff by failing to: (1) adequately protect Customer Data, (2) adequately monitoring data security systems for existing breaches and malware, (3) adequately perform tests to determine the strength of credit and debit card processing systems, (4) adequately training employees to detect and defend against malware intrusions, and (5) adequately testing processing systems using tests from third-party vendors.

48. Wawa's breaches and unlawful conduct directly and proximately caused the theft and dissemination of Plaintiff's and Class members' Customer Data, causing them to suffer, and will continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

(a) Theft of their personal and financial information;

(b) Future unauthorized debit and credit card charges;

(c) Impending injury from potential fraud and identity theft as a result of their PII and PCD being in the hands of hackers, as well as misuse of that data via the sale of Plaintiffs' and Class members' information on the "dark web";

(d) A lack of timely disclosure of the Data Breach;

(e) The loss of privacy;

(f) Money paid for items and gas purchased at Wawa locations during the period of the Data Breach which the Plaintiffs and Class members would not have purchased,

had Wawa disclosed that it maintained inadequate security systems and procedures to reasonably safeguard customers' financial and personal information;

(g) Money paid in the form of out-of-pocket expenses and the value of time lost in attempts to mitigate the damage caused by the Data Breach;

(h) Money lost in the form of cash back or other credit card/debit card benefits as a result of the inability to use certain accounts and cards which were compromised as a result of the Data Breach;

(i) Money lost as a result of loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts, resulting in missed payments on bills and loans, late charges and fees, and adverse effects on their credit (including adverse credit notations); and,

(j) Time and productivity lost as a result of needing to address, attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including the stress, nuisance, and annoyance of dealing with all such issues resulting from the data breach.

49. Although the Customer Data of Plaintiff and the members of the Class has been stolen, Wawa continues to operate meaning it continues to store and acquire millions of customers' PII and PCD after showing a complete inability to prevent a breach from occurring or to identify that a breach has occurred. Plaintiff and members of the Class have an interest in insuring that their data is secure, remains secure, and is promptly destroyed prior to being subject to future theft.

CLASS ACTION ALLEGATIONS

50. Plaintiff seeks relief in his individual capacity and as a representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3), and (c)4, Plaintiff seeks

certification of a Nationwide Class, a Pennsylvania Sub-Class and a Virginia Sub-Class (collectively, the "Classes") defined as follows:

> Nationwide Class: All persons in the United States whose PII was compromised as a result of the Data Breach disclosed on December 19, 2019.
>
> Pennsylvania Sub-Class: All residents of the commonwealth of Pennsylvania whose credit or debit card numbers were compromised in the Data Breach disclosed on December 19, 2019.
>
> Virginia Sub-Class: All residents of the commonwealth of Virginia whose credit or debit card numbers were compromised in the Data Breach disclosed on December 19, 2019.
>
> Excluded from the Classes are: Wawa, including any entity in which Wawa has a controlling interest, is a parent or subsidiary, or which is controlled by Wawa, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Wawa. Also excluded are the judges and court personnel assigned to this case.

51. **Numerosity.** Pursuant to Fed. R. Civ. P. 23(a)(1), the members of the Class are so numerous that joinder of all members is impractical. While the exact number of Class members remains to be unknown to Plaintiff at this time, Wawa has acknowledged that all 850+ locations (serving nearly 400 million customer purchases each year) were affected by the breach, including those shopped at by the Plaintiff.

52. **Commonality.** Pursuant to Fed. R. Civ. P. 23(a)(2) and (b)(3), there are questions of law and of fact which are common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, but are not limited to:

(a) Whether Wawa had a duty to reasonably secure customer PII and PCD, and whether it breached that duty;

(b) Which security procedures and which data breach notification procedures should Wawa be required to implement as part of any injunctive relief ordered by this Court;

(c) Whether Wawa has an implied contractual obligation to use reasonable security measures;

(d) Whether Wawa has complied with any implied contractual obligation to use reasonable security measures;

(e) What security measures must be implemented by Wawa to comply with its implied contractual obligations; and,

(f) What the nature of the relief should be, including equitable relief, to which the Plaintiff and Class members are entitled.

53. All members of the proposed Classes are readily ascertainable. Wawa has access to the addresses and contact information for the (potentially) millions of members of the Classes, which can be used for providing notice to many Class members.

54. **Typicality.** Pursuant to Fed. R. Civ. P. 23(a)(3), Plaintiff's claims are typical of those other Class members, because Plaintiffs' PII and PCD, like that of the other Class members, was inadequately safeguarded through Wawa's uniform misconduct.

55. **Adequacy of Representation**. Pursuant to Fed. R. Civ. P. 23(a)(4), Plaintiff will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation.

56. **Superiority of Class Action**. Pursuant to Fed. R. Civ. P. 23(b)(3), a class action is superior to the other available methods for fair and just adjudication of this controversy since joinder of all the Class members is impracticable. Furthermore, adjudication of this controversy

through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficult in the management of this action as a class action.

57. Pursuant to Fed. R. Civ. P. 23(c)(4), Plaintiff and the Classes seek certification of specific claims and issues in the alternative to certification of all issues and claims.

58. Damages for an individual class member are likely insufficient to justify the cost of individual litigation so that, in the absence to class treatment, Wawa's violations of law inflicting substantial damages in the aggregate would go un-remedied.

59. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2), because Wawa has acted or has refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to each Class as a whole.

COUNT I

Breach of Implied Contract

60. Plaintiff repeats and fully incorporates the allegations already set forth by this complaint.

61. Wawa solicited and invited Plaintiff and the Class members to use its convenience stores and gasoline services. Plaintiff and the Class members accepted Wawa's offer by virtue of going to a Wawa location during the Data Breach period.

62. When Plaintiff and Class members used Wawa's convenience store and gasoline services, they provided their PII and PCD in order to make purchases. In so doing, Plaintiff and the Class members entered into implied contracts with Wawa pursuant to which Wawa agreed to safeguard and protect such information.

63. Each use of Wawa's convenience store and gasoline services was made pursuant to the mutually agreed-upon implied contract with Wawa under which Wawa agreed to safeguard and protect the Plaintiff and Class members' PII and PCD.

64. Plaintiff and the Class members would not have provided or entrusted their PII and PCD to Wawa in the absence of the implied contract between them and Wawa.

65. Plaintiff and Class members fully performed their obligations under the implied contracts with Wawa.

66. As a direct and proximate result of Wawa's breaches of the implied contracts between Wawa and Plaintiff and the Class members, Plaintiff and Class members sustained actual losses and damages as described in detail above.

COUNT II

Negligence

67. Plaintiff repeats and fully incorporates the allegations already set forth by this complaint.

68. Upon accepting and storing Plaintiff and Class members PII and PCD it its computer network, Wawa undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to utilized commercially reasonable methods to do so.

69. Wawa breached its duty to the Plaintiff and the Class members to adequately protect and safeguard this information by disregarding standard information security principles, despite obvious risks, and by allowing the unmonitored and unrestricted access to unsecured PII and PCD.

70. Wawa also failed to provide adequate supervision and oversight of PII and PCD with which it is entrusted, in spite of the known risk and foreseeable likelihood of breach and

misuse, which permitted a third party to gather Plaintiff and other Class members PII and PCD, misuse the PII and PCD, and intentionally disclose it to others without consent.

71. Through Wawa's conduct described in this Complaint, including Wawa's failure to provide adequate security and its failure to protect Plaintiff and Class members PII and PCD from being foreseeably captured, accessed, disseminated, stolen and misused, Wawa unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' PII and PCD during the time it was within Wawa's possession and control.

72. Upon information and belief, Wawa improperly and inadequately safeguarded the PII and PCD of Plaintiff and the Class members in deviation from standard industry rules, regulations, and practices at the time of the Data Breach.

73. Wawa's failure to take proper security measures to protect Plaintiff and Class members' sensitive PII and PCD as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs and Class members' PII and PCD.

74. Wawa's conduct was clearly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII and PCD; failing to conduct regular and/or effective security audits for malware; and failing to provide adequate and appropriate supervision of persons having access to Plaintiff and Class members' PII and PCD.

75. Neither the Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their PII and PCD as described in this Complaint.

76. As a direct and proximate cause of Wawa's conduct, Plaintiffs and Class members suffered damages as alleged above.

COUNT III

PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW

73 Pa. Statute Sect. 201-1 to 201-9.2

77. Plaintiff repeats and fully incorporates the allegations already set forth by this complaint.

78. Plaintiff and Defendant are each a "person" as defined by the statute.

79. Plaintiff and Class members purchased goods and services in "trade" and "commerce" as defined by the statute.

80. Plaintiff and Class members purchased goods and services primarily for personal consumption, for family consumption, and/or for household purposes as defined by the statute.

81. Defendant engaged in "unfair methods of competition" or "unfair or deceptive acts or practices" as defined by the statute by engaging in the following conduct: (a) Representing that goods or services have characteristics, uses, benefits, and qualities that they do not have - specifically, that the goods or services lack adequate data security; (b) Representing that goods and services are of a particular standard or quality when they are not of that standard or quality; and, (c) "engaging in any other deceptive conduct which creates a likelihood of confusion or of misunderstanding" as defined by the statute.

82. These unfair methods of competition and unfair or deceptive acts or practices are declared unlawful by the statute, specifically 73 Pa. Stat. § 201-3.

83. Wawa's unfair or deceptive acts and practices include but are not limited to: (1) failing to implement and maintain reasonable data security measures to protect cardholder information, (2) failing to identify foreseeable data security risks and to address those risks, (3) failing to comply with common law duties, industry standards, and FTC regulations regarding data

security, and, (4) omitting and concealing the material fact that Wawa lacked the necessary measures to safeguard Customer Data.

84. Wawa's representations and omissions were material because they induced reasonable customers to believe in Wawa's representations about their capacity to protect Customer Data.

85. Wawa intended to mislead consumers and induce them to rely on these misrepresentations and omissions.

86. Had Wawa disclosed to customers the inadequacies of their data security systems, Plaintiff and Class members would not have given their data to Wawa and Wawa would have been forced to adopt reasonable data security measures.

87. Plaintiff and the class members acted reasonably in relying on Wawa's misrepresentations and omissions, as they could not ascertain the truthfulness of these statements with mere reasonable diligence.

88. Wawa acted intentionally, knowingly, and maliciously in violating the Pennsylvania Unfair Trade Practices and Consumer Protection law, and recklessly disregarded consumer rights.

89. As a direct and proximate result of Wawa'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 injury, ascertainable losses of money and/or property, and non-monetary damages as described in detail herein.

90. Plaintiff and class members seek all monetary and non-monetary relief as recoverable by law, including the following as expressly permitted by statute: actual damages or

statutory damages of $100 (whichever is greater), treble damages, reasonable attorneys' fees, litigation costs, and such additional relief as the Court deems necessary and proper.

91. As a direct and proximate cause of Wawa's conduct, Plaintiff and Class members suffered damages as alleged above.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class members proposed in this Complaint, respectfully request that the Court enter judgment in his favor and against Wawa as follows:

A. For an Order certifying the Classes as defined here, and appointing Plaintiff and his counsel to represent the Class;

B. For equitable relief enjoining Wawa from engaging in the wrongful conduct complained of here pertaining to the misuse and/or disclosure of Plaintiff's and Class members' PII and PCD, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class members;

C. For equitable relief compelling Wawa to utilize appropriate methods and policies with respect to customer data collection, storage, deletion, and safekeeping and to disclose with specificity to Class members the type of PII and PCD compromised;

D. For equitable relief requiring restitution as applicable;

E. For an award of actual damages and compensatory damages, in an amount to be determined;

F. For an award of costs of suit and attorneys' fees, as allowable by law; and,

G. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial of his claims by jury to the extent authorized by law.

DATED: December 27, 2019

BERGER MONTAGUE, PC

Sherrie R. Savett (PA Bar No. 17646)
Shanon J. Carson (PA Bar No. 85957)
Jon J. Lambiras (PA Bar No. 92384)
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Telephone: (215) 875-3000
Facsimile: (215) 875-4604
Email: ssavett@bm.net
scarson@bm.net
jlambiras@bm.net

MILBERG PHILLIPS GROSSMAN LLP
Michael J. Gallagher, Jr.
Andrei V. Rado (*pro hac vice forthcoming*)
Blake H. Yagman (*pro hac vice forthcoming*)
One Pennsylvania Plaza, Suite 1920
New York, New York, 10119-0165
Telephone: (212) 594-5300
Facsimile: (212) 868-1229
Email: mgallagher@milberg.com
arado@milberg.com
byagman@milberg.com