UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

THERESA A. JACOBS, individually and on behalf of all others similarly situated, Plaintiff, v. WAWA, Inc., Defendant.	Civil Action No. _____ **Class Action Complaint** **Jury Trial Demanded**

CLASS ACTION COMPLAINT

Plaintiff, Theresa A. Jacobs (hereinafter, "Plaintiff"), individually and on behalf of the Class and/or Subclass defined below, alleges the following against Wawa, Inc. ("Wawa" or "Defendant") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THIS CASE

1. Plaintiff brings this class action against Defendant Wawa on behalf of a class (the "Class") and/or subclass ("Subclass") defined below (the "Class" and "Subclass", sometimes referred herein as the "Class").

2. Wawa owns and operates more than 850 convenience stores in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida and Washington, D.C.

3. This action arises from Wawa's failure to properly secure and safeguard consumers' personally identifiable information ("PII") which it collected from its customers at its various locations, and, upon learning of the breach in which this PII was unlawfully obtained,

to provide timely, accurate and adequate notice to Plaintiff and other putative Class or Subclass members that their PII had been stolen, and the types of information that were stolen.

4. On December 19, 2019, Wawa publicly acknowledged that a cybersecurity incident ("Data Breach") affecting most of its stores' systems throughout the country had occurred. It disclosed that malware was discovered on its payment processing servers at potentially all of its locations beginning at different points in time after March 4, 2019 until it was purportedly contained on December 12, 2019. The information accessed primarily includes 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. Wawa has not yet disclosed how many U.S. consumers have been affected by this breach.

5. Wawa acknowledged that it discovered the unauthorized access on December 10, 2019 but failed to inform the public why it delayed notification of the Data Breach to consumers.

6. The PII for Plaintiff and the Class was compromised due to Wawa's acts and omissions and its failure to properly protect the PII.

7. Wawa could have prevented this Data Breach, as the Data Breach was the inevitable result of Wawa's inadequate approach to data security and the protection of the PII that it collected during the course of its business.

8. Wawa disregarded the rights of Plaintiff and Class and/or Subclass members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that it did not have adequate computer systems and/or payment processor servers

and security practices to safeguard PII, failing to take available steps to prevent and stop the breach from ever happening, and failing to monitor and detect the breach on a timely basis.

9. As a result of the Wawa Data Breach, the PII of the Plaintiff and Class members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class members, or likely to be suffered by Plaintiff and Class members as a direct result of the Wawa Data Breach include:

a. unauthorized use of their PII;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PII;

e. loss of use of and access to their account funds and the costs associated with their inability to obtain money from their accounts or being limited in the amount of money they are permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance and annoyance of dealing with all issues resulting from the Wawa Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of criminals and which is already being misused via the sale of Plaintiff's and Class members' information on the Internet black market;

h. damages to and diminution in value of their PII entrusted to Wawa for the sole purpose of purchasing products and services from Wawa; and

i. the loss of Plaintiff's and Class members' privacy.

10. The injuries to the Plaintiff and Class members were directly and proximately caused by Wawa's failure to implement or maintain adequate data security measures for PII.

11. Further, Plaintiff retains a significant interest in ensuring that her PII, which, while stolen, remains in the possession of Wawa, is protected from further breaches, and seeks to remedy the harms she has suffered on behalf of herself and similarly situated consumers whose PII was stolen as a result of the Wawa Data Breach.

12. Plaintiff brings this action to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiff seeks the following remedies, among others: statutory damages under state consumer protection statutes, reimbursement of out-of-pocket losses, other compensatory damages, further and more robust credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Wawa to implement improved data security measures.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative Class

members. And, at least some members of the proposed Class have different citizenship from Wawa.

13. This Court has personal jurisdiction over Plaintiff because Plaintiff submits to the Court's jurisdiction.

14. This Court has personal jurisdiction over Defendant pursuant to 18 U.S.C. § 1965(d) because it is found, has agents, and transacts business in this District and because it has its principal place of business in the State of Pennsylvania.

15. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) and (c)(2) because Defendant's contacts are sufficient to subject it to personal jurisdiction in this District, and therefore, Defendant resides in this District for purposes of venue, or under 28 U.S.C. § 1391(b)(2) because certain acts giving rise to the claims at issue in this complaint ("Complaint") occurred, among other places, in this District.

PARTIES

16. Plaintiff Theresa A. Jacobs is a citizen and resident of the state of New Jersey. She is a victim of the Data Breach. During the relevant period, Ms. Jacobs used her credit card at Wawa convenience stores in order to purchase goods and gift cards, in and around southern New Jersey. Upon information and belief, Plaintiff's PII was compromised as a result of the Data Breach and she has spent time and effort monitoring her financial accounts as a consequence of the Data Breach.

17. Defendant Wawa, Inc. is a New Jersey corporation with its principal place of business located at 260 West Baltimore Pike, Wawa, Pennsylvania 19063.

STATEMENT OF FACTS

18. Wawa is an American chain of convenience stores and gas stations located along the East Coast of the United States, operating in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, and Florida. Wawa has more than 850 convenience retail stores with over 500 offering gasoline.

19. According to Wawa's CEO Chris Gheysen's open letter (the "Letter") to its customers on December 19, 2019, Wawa discovered the data breach on December 10, 2019,[1] when Wawa's information security team discovered malware on Wawa payment processing servers. This malware affected customer payment card information used at potentially all Wawa locations at different points in time after March 4, 2019. Malware began running on in-store payment processing systems at potentially all Wawa locations after March 4, 2019. This malware was present on most store systems by approximately April 22, 2019.

20. The Data Breach was allegedly contained by December 12, 2019. As the Letter states: "[a]t this time, we believe this malware no longer poses a risk to Wawa customers using payment cards at Wawa, and this malware never posed a risk to our ATM cash machines."

21. 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.

22. Plaintiff suffered actual injuries in the form of damages to and diminution in the value of her PII – a form of intangible property that Plaintiff entrusted to Wawa and that was compromised in and as a result of the Wawa Data Breach.

[1] *See* "An Open Letter from Wawa CEO Chris Gheysens to Our Customers", available at https://www.wawa.com/alerts/data-security (last visited December 20, 2019).

23. Additionally, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse because her PII may now be in the hands of criminals who have already, or will imminently, misuse such information.

24. Moreover, Plaintiff has a continuing interest in ensuring that her private information, which remains in the possession of Wawa, is protected and safeguarded from future breaches.

25. At all relevant times, Wawa was well-aware, or reasonably should have been aware, that the PII collected, maintained and stored in the POS systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

26. It is well known and the subject of many media reports that PII is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches of corporate entities, Wawa maintained an insufficient and inadequate system to protect the PII of Plaintiff and Class members.

27. PII is a valuable commodity. A "cyber blackmarket" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. PII is "as good as gold" to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

28. Legitimate organizations and the criminal underground alike recognize the value in PII contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise

the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users."[2]

29. At all relevant times, Wawa knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on individuals as a result of a breach.

30. Wawa was, or should have been, fully aware of the significant number of people whose PII it collected, and thus, the significant number of individuals who would be harmed by a breach of Wawa's systems.

31. As alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, Wawa's approach to maintaining the privacy and security of the PII of Plaintiff and Class members was reckless, or at the very least, negligent.

32. The ramifications of Wawa's failure to keep Plaintiff's and Class members' data secure are severe.

33. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[3] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[4]

34. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have

[2] Verizon 2014 PCI Compliance Report, available at: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54 (last visited December 20, 2019).

[3] 17 C.F.R § 248.201 (2013).

[4] *Id*.

personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[5]

35. Identity thieves can use personal information, such as that of Plaintiff and Class members which Wawa failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

36. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[6]

37. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[7]

38. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

---

[5] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited December 20, 2019).

[6] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited December 20, 2019).

[7] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited December 20, 2019).

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[8]

39. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

40. The PII of Plaintiff and Class members is private and sensitive in nature and was left inadequately protected by Wawa. Wawa did not obtain Plaintiff's and Class members' consent to disclose their PII to any other person as required by applicable law and industry standards.

41. The Wawa Data Breach was a direct and proximate result of Wawa's failure to properly safeguard and protect Plaintiff's and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, 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's and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

42. Wawa had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

[8] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited December 20, 2019).

43. Had Wawa remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, Wawa could have prevented the Data Breach and, ultimately, the theft of its customers' PII.

44. As a direct and proximate result of Wawa's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work, to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

45. Wawa's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' PII, causing them to suffer, and to 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. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and the fact that it is already being misused though the sale of Plaintiff's and Class members' information on the black market;

d. the untimely and inadequate notification of the Data Breach;

e. the improper disclosure of their PII;

f. loss of privacy;

g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

h. ascertainable losses in the form of deprivation of the value of their PII and PCD, for which there is a well-established national and international market;

i. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

j. 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 were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and

k. the loss of productivity and value of their time spent to address attempts to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, the imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

46. Wawa has not offered customers any meaningful credit monitoring or identity theft protection services, despite the fact that it is well known and acknowledged by the government that damage and fraud from a data breach can take years to occur. As a result, Plaintiff and Class members are left to their own actions to protect themselves from the financial

damage Wawa has allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Wawa's actions have created for Plaintiff and Class members, is ascertainable and is a determination appropriate for the trier of fact. Wawa has also not offered to cover any of the damages sustained by Plaintiff or Class members.

47. While the PII of Plaintiff and members of the Class has been stolen, Wawa continues to hold PII of consumers, including Plaintiff and Class members. Particularly because Wawa has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and members of the Class have an undeniable interest in insuring that their PII is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

CLASS ALLEGATIONS

48. Plaintiff seeks relief on behalf of herself and as representatives 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 defined as follows:

> All persons residing in the United States whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Wawa in December 2019 (**the "Nationwide Class"**).

49. Pursuant to Fed. R. Civ. P. 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims under the laws of the State of New Jersey, on behalf of a separate New Jersey State Subclass, defined as follows:

> All persons residing in New Jersey whose personally identifiable information was acquired by unauthorized persons in the data breach announced by Wawa in December 2019 (**the "New Jersey Subclass" or "Subclass"**).

50. Excluded from each of the above Classes and/or Subclasses are Wawa and any of its affiliates, parents or subsidiaries; all employees of Wawa; all persons who make a timely

election to be excluded from the Class; government entities; and the judges to whom this case is assigned and their immediate family and court staff.

51. Plaintiff hereby reserves the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery.

52. The proposed Class and/or Subclass meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3) and (c)(4).

53. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class or Subclass are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class or Subclass members is unknown to Plaintiff at this time, the proposed Class or Subclass includes at least millions (thousands in the case of the Subclass) of individuals whose PII was compromised in the Wawa Data Breach. Class or Subclass members may be identified through objective means. Class or Subclass 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.

54. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class or Subclass members. The common questions include:

a. Whether Wawa had a duty to protect PII;

b. Whether Wawa knew or should have known of the susceptibility of their data security systems to a data breach;

c. Whether Wawa's security measures to protect their systems were reasonable in light of the measures recommended by data security experts;

d. Whether Wawa was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Wawa's failure to implement adequate data security measures allowed the breach to occur;

f. Whether Wawa's conduct constituted a violation of the New Jersey Consumer Fraud Act;

g. Whether Wawa's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiff and Class or Subclass members;

h. Whether Plaintiff and Class or Subclass members were injured and suffered damages or other acceptable losses because of Wawa's failure to reasonably protect its POS systems and data network; and,

i. Whether Plaintiff and Class or Subclass members are entitled to relief.

55. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff's claims are typical of those of other Class or Subclass members. Plaintiff had her PII compromised in the Data Breach. Plaintiff's damages and injuries are akin to other Class or Subclass members and Plaintiff seeks relief consistent with the relief of the Class or Subclass.

56. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Class or Subclass because Plaintiff is a member of the Class or Subclass and is committed to pursuing this matter against Wawa to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class or Subclass. Plaintiff's Counsel are

competent and experienced in litigating class actions, including privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class' or Subclass' interests.

57. **Superiority. Fed. R. Civ. P. 23(b)(3)**. Consistent with Fed. R. Civ. P 23(b)(3), 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 quintessential purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to the individual plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class or Subclass are relatively small compared to the burden and expense required to individually litigate their claims against Wawa, and thus, individual litigation to redress Wawa's wrongful conduct would be impracticable. Individual litigation by each Class or Subclass member would also strain the court system. Individual litigation creates the 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 a single adjudication, economies of scale, and comprehensive supervision by a single court.

58. **Injunctive and Declaratory Relief**. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) and (c). Defendant, through its uniform conduct, has acted or refused to act on grounds generally applicable to the Class or Subclass as a whole, making injunctive and declaratory relief appropriate to the Class or Subclass as a whole.

59. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would

advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Wawa failed to timely notify the public of the Breach;

b. Whether Wawa owed a legal duty to Plaintiff and the Class or Subcclass to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Wawa's security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;

d. Whether Wawa failed to adequately comply with industry standards amounting to negligence;

e. Whether Wawa failed to take commercially reasonable steps to safeguard the PII of Plaintiff and the Class or Subclass members; and,

f. Whether adherence to data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

60. Finally, all members of the proposed Class are readily ascertainable. Wawa has access to information regarding the Data Breach, the time period of the Data Breach, and which individuals were potentially affected. Using this information, the members of the Class or Subclass can be identified and their contact information ascertained for purposes of providing notice to the Class or Subclass .

COUNT I

NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE NEW JERSEY SUBCLASS)

61. Plaintiff re-alleges each and every paragraph above as if fully set forth herein and further alleges as follows.

62. Upon accepting and storing the PII of Plaintiff and Class or Subclass Members in its computer systems, networks, and/or payment processor servers, Wawa undertook and owed a duty to Plaintiff and Class or Subclass Members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Wawa knew that the PII was private and confidential and should be protected as private and confidential.

63. Wawa owed a duty of care not to subject Plaintiff, along with her PII, and Class or Subclass members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

64. Wawa owed numerous duties to Plaintiff and to members of the Nationwide Class or the New Jersey Subclass, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;

b. to protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

65. Wawa also breached its duty to Plaintiff and the Class or Subclass Members to adequately protect and safeguard PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII. Furthering their dilatory practices, Wawa failed to provide adequate supervision and oversight of the PII with which they were and are entrusted, in spite of the known risk and

foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiff and Class or Subclass Members, misuse the PII and intentionally disclose it to others without consent.

66. Wawa knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security. Wawa knew about numerous, well-publicized data breaches.

67. Wawa knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and Class or Subclass Members' PII.

68. Wawa breached its duties to Plaintiff and Class or Subclass Members by failing to provide fair, reasonable, or adequate computer systems and/or payment processor servers and data security practices to safeguard PII of Plaintiff and Class or Subclass Members.

69. Because Wawa knew that a breach of its systems would damage millions of individuals, including Plaintiff and Class or Subclass members, Wawa had a duty to adequately protect their data systems and the PII contained thereon.

70. Wawa had a special relationship with Plaintiff and Class or Subclass members. Plaintiff's and Class or Subclass members' willingness to entrust Wawa with their PII was predicated on the understanding that Wawa would take adequate security precautions. Moreover, only Wawa had the ability to protect its systems and the PII it stored on them from attack.

71. Wawa's own conduct also created a foreseeable risk of harm to Plaintiff and Class or Subclass members and their PII. Wawa's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security

practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

72. Wawa also had independent duties under state and federal laws that required Wawa to reasonably safeguard Plaintiff's and Class or Subclass members' PII and promptly notify them about the data breach.

73. Wawa breached its duties to Plaintiff and Class or Subclass members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and/or payment processor servers and data security practices to safeguard PII of Plaintiff and Class or Subclass members;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiff's and Class or Subclass members' PII both before and after learning of the Data Breach;

d. by failing to comply with the minimum industry data security standards during the period of the Data Breach; and

e. by failing to timely and accurately disclose that Plaintiff's and Class or Subclass members' PII had been improperly acquired or accessed.

74. Through Wawa's acts and omissions described in this Complaint, including Wawa's failure to provide adequate security and its failure to protect PII of Plaintiff and Class or Subclass members from being foreseeably captured, accessed, disseminated, stolen and misused, Wawa unlawfully breached its duty to use reasonable care to adequately protect and secure PII of

Plaintiff and Class or Subclass members during the time it was within Wawa possession or control.

75. The law further imposes an affirmative duty on Wawa to timely disclose the unauthorized access and theft of the PII to Plaintiff and the Class or Subclass so that Plaintiff and Class or Subclass members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

76. Wawa breached its duty to notify Plaintiff and Class or Subclass Members of the unauthorized access by failing to provide Plaintiff and Class or Subclass Members information regarding the breach until December 19, 2019. To date, Wawa has not provided sufficient information to Plaintiff and Class or Subclass Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and the Class or Subclass.

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

78. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Wawa prevented Plaintiff and Class or Subclass Members from taking meaningful, proactive steps to secure their financial data and bank accounts.

79. Upon information and belief, Wawa improperly and inadequately safeguarded PII of Plaintiff and Class or Subclass Members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Wawa's failure to take proper security

measures to protect sensitive PII of Plaintiff and Class or Subclass members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of PII of Plaintiff and Class or Subclass members.

80. Wawa's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to PII of Plaintiff and Class or Subclass members; and failing to provide Plaintiff and Class or Subclass members with timely and sufficient notice that their sensitive PII had been compromised.

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

82. As a direct and proximate cause of Wawa's conduct, Plaintiff and the Class or Subclass suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiff and Class or Subclass Members; damages arising from their inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover

and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

COUNT II

NEGLIGENCE PER SE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE NEW JERSEY SUBCLASS)

83. Plaintiff re-alleges each and every paragraph above as if fully set forth herein and further alleges as follows.

84. 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 PII.

85. Wawa violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Wawa's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach at a corporation such as Wawa, including, specifically, the immense damages that would result to Plaintiff and Class or Subclass Members.

86. Wawa's violation of Section 5 of the FTC Act constitutes negligence per se.

87. Plaintiff and Class or Subclass Members are within the class of persons that the FTC Act was intended to protect.

88. The harm that occurred as a result of the Wawa Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued 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 as that suffered by Plaintiff and the Class or Subclass.

89. As a direct and proximate result of Wawa's negligence per se, Plaintiff and the Class or Subclass have suffered, and continue to suffer, injuries damages arising from their inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

COUNT III

DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE NEW JERSEY SUBCLASS)

90. Plaintiff re-alleges each and every paragraph above as if fully set forth herein and further alleges as follows.

91. As previously alleged, Plaintiff and Class or Subclass members entered into an implied contract that required Wawa to provide adequate security for the PII it collected from

their payment card transactions. As previously alleged, Wawa owes duties of care to Plaintiff and Class or Subclass members that require it to adequately secure PII.

92. Wawa still possesses PII pertaining to Plaintiff and Class or Subclass members.

93. Wawa has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its systems, and only said that the malware was contained.

94. Accordingly, Wawa has not satisfied its contractual obligations and legal duties to Plaintiff and Class or Subclass members. In fact, now that Wawa's lax approach towards data security has become public, the PII in its possession is more vulnerable than previously.

95. Actual harm has arisen in the wake of the Wawa Data Breach regarding Wawa's contractual obligations and duties of care to provide data security measures to Plaintiff and Class or Subclass members.

96. Plaintiff, therefore, seeks a declaration that (a) Wawa's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Wawa must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Wawa's systems on a periodic basis, and ordering Wawa to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting PII by, among other things, creating firewalls and access controls so that if one area of Wawa is compromised, hackers cannot gain access to other portions of Wawa systems;

e. purging, deleting, and destroying in a reasonably secure manner PII not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Wawa customers must take to protect themselves.

COUNT IV

VIOLATIONS OF THE NEW JERSEY CONSUMER FRAUD ACT, N.J. STAT. ANN. §56:8-2, *et seq.* (ON BEHALF OF PLAINTIFF AND THE NEW JERSEY SUBCLASS)

97. Plaintiff repeats and realleges each and every paragraph above as if fully set forth herein and further alleges as follows.

98. Plaintiff brings this claim for relief individually and on behalf of the New Jersey Subclass pursuant to New Jersey Consumer Fraud Act, N.J. Stat. Ann. §56:8-2, *et seq*. ("NJCFA").

99. By engaging in the conduct alleged in this Complaint, Wawa intended to and did engage in the sale of "merchandise" to consumers as defined by NJCFA.

100. Wawa's relevant acts, practices and omissions complained of in this action were done in the course of Wawa's business of marketing, offering for sale and selling food products, gasoline, goods and services throughout the State of New Jersey and the Eastern United States.

101. The NJCFA, prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the State of New Jersey.

102. In the conduct of its business, trade, and commerce, and in the sale of food products, gasoline, goods or services to consumers in the State of New Jersey, Wawa collected and stored highly personal and private information, including sensitive financial information of Wawa's customers, like Plaintiff and member of the putative Subclass.

103. Wawa knew or should have known that its computer systems and data security practices were inadequate to safeguard the sensitive financial information of the Subclass and that the risk of data breach was highly likely and/or that the risk of the data breach being more extensive than originally disclosed was highly likely.

104. Wawa should have disclosed this information regarding its computer systems and data security practices because Wawa was in a superior position to know the true facts related to its security vulnerability, and members of the Subclass could not reasonably be expected to learn or discover the true facts.

105. As alleged throughout this Complaint, Wawa's deliberate conduct constitutes deceptive, unfair and unlawful trade acts or practices in the conduct of trade or commerce and the furnishing of services in the State of New Jersey, in violation of the NJCFA, including but not limited to its:

a. Failure to maintain adequate computer systems and/or payment processor servers and data security practices to safeguard consumers' PII;

b. Failure to disclose that its computer systems and/or payment processor servers and data security practices were inadequate to safeguard consumers' PII from theft;

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

d. Failure to timely and accurately disclose the data breach to Plaintiff and other members of the Subclass and knowingly omitting, suppressing, and concealing the material fact that Wawa's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft, with the intent that others rely upon the omission, suppression, and concealment;

e. Continued acceptance of PII and storage of other personal information after Wawa knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach; and

f. Continued acceptance of PII and storage of other personal information after Wawa knew or should have known of the Data Breach and before it allegedly remediated the Breach.

106. Plaintiff and other members of the Subclass relied upon Wawa's deceptive and unlawful conduct, and Wawa's conduct was negligent, knowing and willful and/or wanton and reckless with respect to the Subclass.

107. Plaintiff and other members of the Subclass entrusted Wawa with their PII.

108. As a direct and proximate result of Wawa's violation of the NJCFA, members of the New Jersey Subclass have suffered ascertainable losses of money and actual damages, including, inter alia:

a. Fraudulent charges on their debit and credit card accounts which may not be reimbursed;

b. Theft of their PII by criminals;

c. Costs associated with the detection and prevention of identity theft;

d. Costs associated with the fraudulent use of their financial accounts;

e. Loss of use of and access to some or all of their account funds and costs incurred as a result of being unable to access those funds;

f. Costs and time associated with handling the administrative consequences of the Wawa data breach, including identifying, disputing and seeking reimbursement for fraudulent charges, cancelling and activating payment cards, and shopping for credit monitoring and identity theft protection;

g. Impairment of their credit scores and ability to borrow and/or obtain credit;

h. The continued risk to their PII which remains on Wawa's insufficiently secured systems; and

i. The continued risk to their personal information, which has been accessible to criminals for over nine months and which remains on Wawa's insufficiently secured computer systems.

109. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of Wawa alleged herein, the Subclass seeks relief under N.J. Stat. Ann. §56:8-19,

including, but not limited to, actual damages, treble damages, injunctive relief, and attorneys' fees and costs.

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

COUNT V

UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS, OR, ALTERNATIVELY, PLAINTIFF AND THE NEW JERSEY SUBCLASS)

111. Plaintiff repeats and realleges each and every allegation set forth above as if fully set forth herein. This count is an alternative to the count for a breach of an implied contract.

112. Plaintiff and members of the Class or Subclass conferred a monetary benefit upon Wawa in the form of monies paid for the purchase of food and food-related service at its locations.

113. Wawa appreciated or had knowledge of the benefits conferred upon the Plaintiff and the Class or Subclass. Wawa also benefitted from the receipt of Plaintiff's and the Class's or Subclass's credit card information, as this was utilized by Wawa to facilitate payment to it.

114. The monies that Plaintiff and the Class or Subclass members paid to Wawa were supposed to be used by Wawa, in part, to pay for adequate data privacy infrastructures, practices, and procedures.

115. As a result of Wawa's conduct, Plaintiff and members of the Class or Subclass suffered actual damages in an amount equal to the difference in value between their purchases made with adequate data privacy and security practices and procedures that Plaintiff and Class or Subclass members paid for, and those purchases without adequate data privacy and security practices and procedures that they received.

116. Under principals of equity and good conscience, Wawa should not be permitted to retain the money belonging to Plaintiff and Class or Subclass members because Wawa failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class or Subclass members paid for and that were otherwise mandated by federal, state, and local laws, and industry standards.

117. Wawa should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class or Subclass members all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

REQUEST FOR RELIEF

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

a. For an Order certifying the Class (or Subclass), as defined herein, and appointing Plaintiff and her Counsel to represent the Nationwide Class, or in the alternative the New Jersey Subclass;

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

c. For equitable relief compelling Wawa to use appropriate cyber security methods and policies with respect to consumer data collection, storage and protection and to disclose with specificity to Class members the type of PII compromised;

d. For an award of damages, as allowed by law in an amount to be determined;

e. For an award of attorneys' fees costs and litigation expenses, as allowable by law;

f. For prejudgment interest on all amounts awarded; and

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

JURY TRIAL DEMANDED

Plaintiff demands a jury trial on all issues so triable.

Dated: January 3, 2020

Respectfully Submitted:

Jonathan Shub (PA ID 53965)
Kevin Laukaitis (PA ID 321670)
KOHN, SWIFT & GRAF, P.C.
160 Market Street, Suite 2500
Philadelphia, PA 19103
Phone: (215) 238-1700
jshub@kohnswift.com
klaukaitis@kohnswift.com

Lynda J. Grant, Esq.*
THEGRANTLAWFIRM, PLLC
521 Fifth Avenue, 17th Floor
New York, NY 10016
Phone: (212) 292-4441
lgrant@grantfirm.com
**Pro Hac Vice* Application forthcoming

Attorneys for Plaintiff and the Putative Class