$400 JHS

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

SUZANNE HIGH, individually and on behalf of all others similarly situated, Plaintiff, v. WAWA, INC. Defendant.	Case No.: 20 cv 1 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

FILED
JAN - 1 2020
JL

Plaintiff Suzanne High ("Plaintiff"), individually and on behalf of Classes defined below of similarly situated persons, brings this Complaint and alleges the following against Wawa Inc. ("Wawa" or "Defendant"), based upon personal knowledge as to herself, and on information and belief as to all other matters.

NATURE OF THE ACTION

1. This is a putative class action lawsuit brought against Wawa for its failure to properly secure and safeguard the payment card data ("PCD") and personally identifiable information ("PII") (collectively "Customer Data") of its on-line customers and for its failure to provide them timely, accurate and adequate notice that such information had been compromised.

2. On or about December 19, 2019, Wawa publicly revealed that customers' payment card information, including name, address, credit card number, expiration date, and security code (CVD)" had be compromised, accessed and subsequently stolen by an unauthorized third party ("Data Breach").

3. According the announcement made by CEO Chris Gheysens, the company discovered on December 10, 2019 that malware was running on its payment processing servers stealing payment card information since March 4, 2019. The malware affected potentially all

l

Wawa locations beginning at different times after March 4. 2019, with most locations affected as of April 22, 2019.

4. Wawa disregarded the rights of Plaintiff and Class members[1] by: intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected; failing to disclose the material fact that it neither had adequate security practices, nor sufficient safeguards in place to protect the Customer Data with which it was entrusted; failing to take available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiff and putative class members prompt and accurate notice of the Data Breach.

5. As a result of Defendant's failure to implement and follow standard security procedures Plaintiff's and Class members' Customer Data is in the hands of thieves. As a result of Defendant's basic failures Plaintiff and Class members now face an increased risk of identity theft and will have to spend significant amounts of time and money to protect themselves. Indeed, Plaintiff has already suffered financial harm and adverse credit events as a result of the Data Breach and has expended significant amounts of time in an effort to mitigate its deleterious effects.

6. Plaintiff, on behalf of herself and classes of similarly situated individuals, seeks to remedy the harms suffered as a result of the Data Breach and to ensure that the Customer Data, which remains in the possession of Defendant, is protected from further breaches.

7. Defendant's conduct gives rise to claims for negligence, negligence per se, breach of implied contract, breach of fiduciary duty, breach of confidence, breach of privacy and is in violation of Florida's Deceptive and Unfair Trade Practices Act and Pennsylvania's Unfair Trade

[1] See, Infra at ¶66.

Practices and Consumer Protection Law. Plaintiff, individually, and on behalf of those similarly situated, seeks damages, equitable relief, injunctive relief, restitution, and all other remedies this Court deems proper.

JURISDICTION AND VENUE

8. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act 28 U.S.C. § 1332(d) ("CAFA"), as the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs, there are more than 100 Class members, and at least one class Member is a citizen of a state different from Defendant.

9. This Court has personal jurisdiction over Defendant because Wawa is incorporated in Pennsylvania, regularly conducts business in this District, and maintains its principal place of business in this District.

10. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because the Defendant's principal places of business is in this District and a substantial part of the events or omissions giving rise to this action, particularly decisions related to data security and the acts which lead to the Data Breach, occurred in this District.

PARTIES

11. Plaintiff Suzanne High is a citizen and resident of Osceola County, Florida. Ms. High is a regular shopper and customer of Wawa. During the time frame of the Data Breach, Ms. High would make purchases from Wawa at least once a month. She typically used a debit card issued by Bank of America. In or around August of 2019, Ms. High was notified that her debit card had been compromised and fraudulent charges had been made on her account

12. On information and belief, as a direct result of the Data Breach, Plaintiff's Customer Data was compromised.

13. As a result of the Data Breach, Ms. High was required to spend time working with her bank to have the fraudulent charges reversed and a new debit card issued. As a result of the Data Breach, Ms. High was required to spend hours of time contacting her payees with new debit card information and continues to spend her valuable time to protect the integrity of her finances and credit – time which she would not have had to expend but for the Data Breach.

14. Defendant Wawa is a privately held company with its principal place of business located in Wawa, Pennsylvania. It operates a chain of more than 750 convenience retail stores located across Pennsylvania, New Jersey, Delaware, Maryland, Virginia, and Florida.

FACTUAL ALLEGATIONS

A. The Wawa Data Breach

15. On or about December 10, 2019, Defendant's information security team discovered malware on the company's payment processing servers. The company has announced that an unauthorized third party gained access to Wawa Customer Data including, names, addresses, credit card numbers, credit card expiration dates and security codes.

16. On December 19, 2019, Defendant publicly announced that its Customer Data had been exposed and compromised. In the notice, Wawa's CEO stated as follows:

> At Wawa, the people who come through our doors every day are not just customers, you are our friends and neighbors, and nothing is more important than honoring and protecting your trust. Today, I am very sorry to share with you that Wawa has experienced a data security incident. Our information security team discovered malware on Wawa payment processing servers on December 10, 2019, and contained it by December 12, 2019. This malware affected customer payment card information used at potentially all Wawa locations beginning at different points in time after March 4, 2019 and until it was contained. At 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.
> 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.

What Happened?

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. We also immediately initiated an investigation, notified law enforcement and payment card companies, and engaged a leading external forensics firm to support our response efforts. Because of the immediate steps we took after discovering this malware, we believe that as of December 12, 2019, this malware no longer poses a risk to customers using payment cards at Wawa.

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. Most locations were affected as of April 22, 2019, however, some locations may not have been affected at all. No other personal information was accessed by this malware. Debit card PIN numbers, credit card CVV2 numbers (the three or four-digit security code printed on the card), other PIN numbers, and driver's license information used to verify age-restricted purchases were not affected by this malware. If you did not use a payment card at a Wawa in-store payment terminal or fuel dispenser during the relevant time frame, your information was not affected by this malware. At this time, we are not aware of any unauthorized use of any payment card information as a result of this incident. The ATM cash machines in our stores were not involved in this incident.

What We Are Doing

As soon as we discovered this malware on December 10, 2019, we took immediate steps to contain it, and by December 12, 2019, we had blocked and contained it. We believe this malware no longer poses a risk to customers using payment cards at Wawa. As indicated above, we engaged a leading external forensics firm to conduct an investigation, which has allowed us to provide the information that we are now able to share in this letter. We are also working with law enforcement to support their ongoing criminal investigation. We continue to take steps to enhance the security of our systems. We have also arranged for a dedicated toll-free call center (1-844-386-9559) to answer customer questions and offer credit monitoring and identity theft protection without charge to anyone whose information may have been involved, which you can sign up for as described below.

What You Can Do

Customers whose information may have been involved should consider the following recommendations, all of which are good data security precautions in general:

- Review Your Payment Card Account Statements. We encourage you to remain vigilant by reviewing your payment card account statements. If you believe there is an unauthorized charge on your payment card, please notify the relevant payment card company by calling the number on the back of the card. Under federal law and card company rules, customers who notify their payment card company in a timely manner upon discovering fraudulent charges will not be responsible for those charges.
- Register for Identity Protection Services. We have arranged with Experian to provide potentially impacted customers with one year of identity theft protection and credit monitoring at no charge to you. Information about these services is available at www.wawa.com/alerts/data-security or call toll-free to 1-844-386-9559.
- Order a Credit Report. If you enroll in the Experian service (at the phone number above) we are offering, you will have access to activity on your credit report. In addition, if you are a U.S. resident, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228.
- Review the Reference Guide. The Reference Guide below provides additional resources on the protection of personal information.

For More Information

> If you have any questions about this issue or enrolling in the credit monitoring services we are offering at no charge to you, please call our dedicated Experian response phone line at 1-844-386-9559. It is open Monday - Friday, between 9:00 am and 9:00 pm Eastern Time, or Saturday and Sunday, between 11:00 am and 8:00 pm Eastern Time, excluding holidays (which include December 24, December 25, December 31, January 1, and January 20).
>
> Along with the nearly 37,000 Wawa associates in all of our communities, we remain dedicated to serving you every day and being worthy of your continued trust.
>
> Sincerely,
> Chris Gheysens

B. Security Breaches Lead to Identity Theft

17. Customer Data has become a valuable commodity among computer hackers. Once obtained, it is quickly sold on the black market where it can often be re-traded among miscreants for years.[2] Customer Data is particularly valuable to identity thieves who can use victims' personal data to open new financial accounts, take out loans, incur charges, or clone ATM, debit, and credit cards. As reported by the Identity Theft Resource Center, there were 1,579 data breaches in 2017, representing a 44.7 percent increase over the then-record high figures reported for 2016.[3]

18. Professionals tasked with trying to stop fraud and other misuse know that Customer Data has real monetary value as evidenced by criminals' relentless efforts to obtain this data.[4]

---

[2] *Guide for Assisting Identity Theft Victims*, FTC (Sep. 2013), *available at*: https://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (the "FTC Guide").
[3] *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/2017-data-breaches, (last visited December 20, 2019).
[4] *Data Breaches Rise as Cybercriminals Continue to Outwit IT*, *CIO Magazine*, https://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html (last visited December 20, 2019).

Experian reports that a stolen credit or debit card number can sell for $5-110 on the dark web[5] and a complete set of bank account credentials can fetch a thousand dollars or more (depending on the associated credit score or balance available to criminals).[6]

DEFENDANT'S PRIVACY POLICIES AND PROMISES TO KEEP CUSTOMER DATA CONFIDENTIAL

19. As a condition of masking purchases at Wawa using payment cards, Defendant required its customers to provide them with certain personal information including their names, addresses, and credit card information. This information was subsequently maintained by Wawa in the ordinary course of its business.

20. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the Class members' PII and PCD, Defendant assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting Plaintiff's and Class members' PII and PCD from disclosure.

21. At all relevant times, Plaintiff and the Class members have taken reasonable steps to maintain the confidentiality of their PII and PCD. Plaintiff and the Class members, as current and former customers, relied on Defendant to keep their PII and PCD confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. ("Wawa is fully committed to data security.")[7]

---

[5] *Here's How Much Your Personal Information Is Selling for on the Dark Web* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/, (last visited December 20 , 2019).

[6] *Here's How Much Thieves Make By Selling Your Personal Data Online, Business Insider,* http://www.businessinsider.com/heres-how-much-your-personal-data-costs-on-the-dark-web-2015-5, May 27, 2015.

[7] See, Wawa Privacy Policy, available at https://www.wawa.com/privacy (last visited December 19, 2019)

22. Wawa is acutely aware of its legal obligations to maintain the privacy and sanctity of Customer Data with which it is entrusted. It is also acutely aware of the ramifications for the failure to do so. Indeed, as recently as May of 2019, Wawa reassured its customers that protecting customer privacy was important to the company.[8]

23. Despite espousing the importance of securing its customer data, however, Wawa failed to implement or maintain the most basic procedures and protocols necessary to achieve this goal.

WAWA FAILED TO COMPLY WITH INDUSTRY STANDARDS

24. The major payment card industry brands typically set forth specific security measures in their Card Operating Regulations which are binding on merchants such as Wawa and require them to: (1) protect cardholder data and prevent its unauthorized disclosure; (2) store data, even in encrypted form, no longer than necessary to process the transaction; and (3) comply with all industry standards.

25. The Payment Card Industry Data Security Standard ("PCI DSS") is an information security standard for organizations that handle branded credit cards. The standard was created to increase controls around cardholder data to reduce credit card fraud.[9] Compliance with PCI DSS is mandated by credit card companies.

26. The PCI DSS "was developed to encourage and enhance cardholder data security" by providing "a baseline of technical and operational requirements designed to protect account

---

[8] See, Wawa Privacy Policy, available at https://www.wawa.com/privacy (last visited December 19, 2019).

[9] *Payment Card Industry Data Security Standard* available at https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss (last visited December 20, 2019).

data."[10] PCI DSS sets the minimum level of what must be done, not the maximum.

27. PCI DSS requires the following: [11]

PCI Data Security Standard – High Level Overview

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

28. Among other things, PCI DSS required Wawa to properly secure and protect payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; protect systems against malware; regularly test security systems; establish a process to identify and timely fix security vulnerabilities; and encrypt payment card data at the point of sale.

29. Although it was well aware of its data security obligations, Wawa's treatment of PCD and PII fell far short of its legal obligations to protect Customer Data. Wawa failed to ensure that access to its data systems was reasonably safeguarded, failed to acknowledge and act upon industry warnings and failed to use proper security systems to detect and deter the type of attack that occurred and is at issue here. Cumulatively, its failures resulted in the Data Breach.

[10] *Id.*
[11] *Id.*

WAWA FAILED TO COMPLY WITH FTC REQUIREMENTS

30. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guidelines for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[12]

31. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[13] The guidelines note 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 to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting 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. Embracing standard industry practices, the FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party

---

[12] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited December 20 , 2019).

[13] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited December 20, 2019).

service providers have implemented reasonable security measures.[14]

33. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

34. Wawa's failure to employ reasonable and appropriate measures 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. § 45.

35. In this case, Wawa was at all times fully aware of its obligation to protect the financial data of Wawa's customers because of its participation in payment card processing networks. Wawa was also aware of the significant repercussions if it failed to do so because Wawa collected payment card data from tens of thousands of customers daily and they knew that this data, if hacked, would result in injury to consumers, including Plaintiff and Class members.

36. Despite understanding the consequences of inadequate data security, Wawa failed to comply with PCI DSS requirements, FTC Guidelines and standard industry practices designed to ensure the integrity of PII and PCD.

WAWA'S FAILURE TO TIMELY DETECT AND WARN OF THE DATA BREACH CAUSED ADDITIONAL HARM

37. The FTC defines identity theft as "a fraud committed or attempted using the

[14] FTC, *Start With Security*, *supra* note 12.

identifying information of another person without authority."[15] 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."[16]

38. Personal identifying information is a valuable commodity to identity thieves. As the FTC recognizes, once identity thieves have 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."[17]

39. 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.

40. Compounding Wawa's failure to protect Customer Data, was the fact that it failed to detect the breach for at least nine months and, thus, failed to timely inform affected customers that their PCD and PII had been illegally exposed. A 2016 survey of 5,028 consumers found "[t]he quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."[18]

41. As a result of Wawa's delay in detecting the Breach and notifying consumers of the

---

[15] 17 C.F.R § 248.201 (2013).
[16] *Id.*
[17] 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).
[18] *Identity Fraud Hits Record High with 15.4 Million U S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, February 1, 2017, available at https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new (last visited December 20, 2019).

Data Breach, allowing Customer Data to be exposed and compromised for at least nine months, the risk of fraud for Plaintiff and Class members has been driven even higher.

HARM CAUSED BY THE DATA BREACH IS ONGOING

42. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[19]

43. 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.[20]

44. An independent financial services industry research study conducted for BillGuard - a private enterprise that automates the consumer task of finding unauthorized transactions that might otherwise go undetected -calculated the average per-consumer cost of all unauthorized transactions at roughly US $215 per cardholder incurring these charges[21], some portion of which could go undetected and thus must be paid entirely out-of-pocket by consumer victims of account or identity misuse.

45. There may be a time lag between when harm occurs versus when it is discovered,

---

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

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

[21] Hadley Malcom, *Consumers rack up $14.3 billion in gray charges, research study commissioned for Billguard by Aite Research, USA Today* (July 25, 2013), available at: https://www.usatoday.com/story/money/personalfinance/2013/07/25/consumers-unwanted-charges-in-billions/2568645/ (last visited December 20, 2019).

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:

> [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.[22]

46. Thus, Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and the Class are incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred by them and the resulting loss of use of their credit and access to funds, regardless of whether such charges are ultimately reimbursed by banks and credit card companies.

PLAINTIFF AND THE CLASSES SUFFERED DAMAGES

47. The Customer Data belonging to Plaintiff and Class members is private and sensitive in nature and was left inadequately protected by the Defendant. Defendant did not obtain Plaintiff's or Class members' consent to disclose their Customer Data to any other person as required by applicable law and industry standards.

48. The Data Breach was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiff's and Class members' Customer Data from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Defendant's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' Customer Data to protect against reasonably foreseeable threats to

---

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

the security or integrity of such information.

49. According to year end data breach statistics compiled by the Identity Theft Resource Center, of the 1,244 breaches reported in 2018, 571 were attributed to businesses, making them the most targeted group by data hackers.[23]

50. Defendant was acutely aware of the dangers of data breaches and that customer retail data was a particularly high value target. Defendant had the resources necessary to prevent such a breach yet neglected to adequately invest in data security. Defendant designed and implemented their policies and procedures regarding the security of Customer Data. These policies and procedures failed to adhere to reasonable and best industry practices in safeguarding protected PII and PCD.

51. Affected individuals face a real, concrete, and actual risk of harm and future identity theft as the PCD and PII contained confidential biographical information. Had Defendant remedied the deficiencies in its data security systems, adopted security measures recommended by experts in the field, Defendant would have prevented the intrusion and, ultimately, the theft of PCD and PII belonging to Wawa customers.

52. As a direct and proximate result of Defendant's wrongful actions and inaction, 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 and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by their financial institutions, closing or modifying financial accounts, closely reviewing and

[23] https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf (last visited December 20, 2019)

monitoring their credit reports and accounts for unauthorized activity, placing "freezes" and "alerts" with credit reporting agencies, contacting, and filing police reports. This time has been lost forever and cannot be recaptured.

53. Notwithstanding the seriousness of the Data Breach, the Defendant have not offered to provide Plaintiff nor Class members any meaningful assistance or compensation for the costs and burdens—current and future– associated with the unauthorized exposure of their PII.

54. Other than providing generic advice on what to do when one's PII has been exposed in a data breaches, and a free credit report, which is already available to every U.S. consumer, Defendant frugally offered one year free credit monitoring with Experian's IdentityWorks.

55. Defendant' meager credit monitoring offer places the onus on Plaintiff and Class members, rather than Defendant, to investigate and protect themselves from Defendant' tortious acts that resulted in the Data Breach.

56. Although credit monitoring can help detect fraud after it has already occurred, it has very little value as a preventive measure. As noted by security expert Brian Krebs, "although [credit monitoring] services may alert you when someone opens or attempts to open a new line of credit in your name, most will do little — if anything — to block that activity. My take: If you're being offered free monitoring, it probably can't hurt to sign up, but you shouldn't expect the service to stop identity thieves from ruining your credit."[24]

57. As a result of the Defendant' failures to prevent the Data Breach, Plaintiff and Class members have suffered and will continue to suffer damages. They have suffered, or are at increased risk of suffering.

---

[24] *Krebs on Security*, March 19, 2014, https://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it/ (last visited on December 20, 2019)

a. The compromise, publication, theft and/or unauthorized use of their PCD/PII;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

d. The continued risk to their PCD/PII, which remains in the possession of the Defendant and is subject to further breaches so long as the Defendant fails to undertake appropriate measures to protect the PCD/PII in their possession; and

e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of Plaintiff's and Class members' lives.

58. Additionally, Defendant continues to hold the PCD/PII of its customers. Particularly, because Defendant has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class members have an undeniable interest in ensuring that their PCD/PII is secure, remains secure, and is not subject to further theft.

59. Defendant disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that their PCD/PII was safeguarded; failing to take available steps to prevent an unauthorized disclosure of data; and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the

result, the PCD/PII of Plaintiff and Class members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe. In addition to damages, Plaintiff and Class members are entitled to injunctive and other equitable relief.

CLASS ACTION ALLEGATIONS

60. Plaintiff brings this suit as a class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure. Plaintiff seeks certification of a Nationwide Class and Florida Subclass defined as follows:

> **All persons residing in the United States who used a payment card at Wawa for purchases during the period of the Data Breach (the "Nationwide Class").**
>
> **All persons residing in the state of Florida who used a payment card at Wawa for purchases during the period of the Data Breach (the "Florida Subclass").**

61. Excluded from the Class and Subclass are the officers, directors, and legal representatives of Defendant, and the judges and court personnel in this case and any members of their immediate families.

62. Numerosity. Fed. R. Civ. P. 23(a)(1). The Class members are so numerous that joinder of all Members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, the Data Breach affected 850 locations and at least tens of thousands of Wawa customers. The exact number is generally ascertainable by appropriate discovery as Defendant has knowledge of the customers whose PCD/PII was breached.

63. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and

fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether and to what extent Defendant had a duty to protect the PCD/PII of Class members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class members' PCD/PII;

c. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class members' PCD/PII;

d. Whether Defendant failed to adequately safeguard the PCD/PII of Class members;

e. Whether Defendant breached its duty to exercise reasonable care in handling Plaintiff's and Class members' PCD/PII;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

g. Whether implied contracts existed between Wawa, on the one hand, and Plaintiff and Class members on the other;

h. Whether Defendant had respective duties not to use the PCD/PII of Class members for non-business purposes;

i. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PCD/PII of Class members;

j. Whether Class members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiff and Class members are entitled to restitution as a result of

Defendant' wrongful conduct; and,

l. Whether Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

64. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class members because Plaintiff's PCD/PII, like that of every other Class member, was disclosed by Defendant. Plaintiff's claims are typical of those of the other Class members because, *inter alia*, all Members of the Class were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class members, and there are no defenses that are unique to Plaintiff. Plaintiff's claims and those of Class members arise from the same operative facts and are based on the same legal theories.

65. Policies Generally Applicable to the Class. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

66. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class in that she has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages she has suffered are typical of other Class members. Plaintiff has retained counsel

experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

67. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

68. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

69. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

70. Adequate notice can be given to Class members directly using information maintained in Defendant's records.

71. Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

72. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PCD/PII of Class members, Defendant may continue to refuse to provide proper notification to Class members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

73. 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 Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and safeguarding their PCD/PII;

b. Whether Defendant breached a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and safeguarding their PCD/PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant and the Class and the terms of that implied contract;

e. Whether Wawa breached the implied contract;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

g. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PCD/PII of Class members; and,

h. Whether Class members are entitled to actual damages, statutory damages, injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of the Nationwide Class and Florida Subclass)

74. Plaintiff restates and realleges paragraphs 1 through 73 above as if fully set forth herein.

75. As a condition of utilizing Wawa's services customers were obligated to provide Defendant with certain PCD/PII, including their names, addresses, credit card numbers, credit card expiration dates and CVV.

76. Plaintiff and the Class members entrusted their PCD/PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PCD/PII for business purposes only, and/or not disclose their PCD/PII to unauthorized third parties.

77. Defendant has full knowledge of the sensitivity of the PCD/PII and the types of harm that Plaintiff and Class members could and would suffer if the PCD/PII were wrongfully disclosed.

78. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of their customers' PCD/PII involved an unreasonable risk of harm to Plaintiff and Class members, even if the harm occurred through the criminal acts of a third party.

79. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff and Class members' information in Defendant's possession was adequately secured and protected, and that employees tasked with maintaining such information were adequately trained on security measures regarding the security of customers' personal and medical information.

80. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class members' PCD/PII.

81. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class members was reasonably foreseeable, particularly in light of Defendant's inadequate information security practices.

82. Plaintiff and the Class members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew of should have known of the inherent risks in collecting and storing the PCD/PII of Plaintiff and the Class, the critical importance of providing adequate security of that PCD/PII, and that it had inadequate employee

training and education and IT security protocols in place to secure the PCD/PII of Plaintiff and the Class.

83. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PCD/PII of Plaintiff and Class members.

84. Plaintiff and the Class members had no ability to protect their PCD/PII that was in Defendant's possession.

85. Defendant was in a position to protect against the harm suffered by Plaintiff and Class members as a result of the Data Breach.

86. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PCD/PII of Plaintiff and Class members.

87. Defendant has admitted that the PCD/PII of Plaintiff and Class members was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

88. Defendant, through their actions and/or omissions, unlawfully breached its duties to Plaintiff and Class members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PCD/PII of Plaintiff and Class members during the time the PCD/PII was within Defendant's possession or control.

89. Defendant improperly and inadequately safeguarded the PCD/PII of Plaintiff and Class members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

90. Defendant failed to heed industry warnings and alerts to provide adequate

safeguards to protect customers' PCD/PII in the face of increased risk of theft.

91. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of their customers' PCD/PII.

92. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class members the existence and scope of the Data Breach.

93. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class members, the PCD/PII of Plaintiff and Class members would not have been compromised.

94 There is a close causal connection between Defendant's failure to implement security measures to protect the PCD/PII of current and former customers, and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and Class members' PCD/PII was stolen and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PCD/PII by adopting, implementing, and maintaining appropriate security measures and encryption.

95. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PCD/PII is used; (iii) the compromise, publication, and/or theft of their PCD/PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PCD/PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) costs associated

with placing freezes on credit reports; (vii) the continued risk to their PCD/PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PCD/PII of customers in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PCD/PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members; and (ix) the diminished value of Defendant's goods and services they received.

96. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

SECOND CAUSE OF ACTION
Invasion of Privacy
(On Behalf of the Nationwide Class and Florida Subclass)

97. Plaintiff restates and realleges paragraphs 1 through 73 above as if fully set forth herein.

98. Plaintiff and Class members had a legitimate expectation of privacy to their PCD/PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

99. Defendant owed a duty to Wawa customers, including Plaintiff and Class members, to keep their PCD/PII confidential.

100. Defendant failed to protect and released to unknown and unauthorized third parties data containing the PCD/PII of Plaintiff and Class members.

101. Defendant allowed unauthorized and unknown third parties access to and examination of the PCD/PII of Plaintiff and Class members, by way of Defendant's failure to protect the PCD/PII in its databases.

102. The unauthorized release to, custody of, and examination by unauthorized third parties of the PCD/PII of Plaintiff and Class members is highly offensive to a reasonable person.

103. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class members disclosed their PCD/PII to Defendant as part of their use of Defendant's services, but privately with an intention that the PCD/PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

104. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff and Class members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

105. Defendant acted with a knowing state of mind when it permitted the Data Breach because it was with actual knowledge that its information security practices were inadequate and insufficient.

106. As a proximate result of the above acts and omissions of Defendant, the PCD/PII of Plaintiff and Class members was disclosed to third parties without authorization, causing Plaintiff and Class members to suffer damages.

107. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class members in that the PCD/PII maintained by Defendant can be viewed, distributed, and used by unauthorized

persons. Plaintiff and Class members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of the Nationwide Class and Florida Subclass)

108. Plaintiff restates and realleges paragraphs 1 through 73 above as if fully set forth herein.

109. Plaintiff and Class members were required to provide their PCD/PII, including their names, addresses, credit card numbers, expirations dates and security codes to Defendant as a condition of purchasing products through Defendant's website.

110. Plaintiff and Class members paid money to Wawa in exchange for goods and services, as well as Defendant's promises to protect their PCD/PII from unauthorized disclosure.

111. In its written privacy policy, Defendant promised Plaintiff and Class members that it would only disclose PCD/PII under certain circumstances, none of which relate to the Data Breach.

112. Implicit in the agreement between the Defendant and its customers, including Plaintiff and Class members, was Defendant's obligation to use Customer Data for business purposes only, take reasonable steps to secure and safeguard Customer Data, and not make unauthorized disclosures of such data to unauthorized third parties.

113. Further, implicit in the agreement, Defendant was obligated to provide Plaintiff and Class members with prompt and sufficient notice of any and all unauthorized access and/or theft of their protected PCD/PII.

114. Without such implied contracts, Plaintiff and Class members would not have

provided their PCD/PII to Defendant.

115. Defendant had an implied duty to reasonably safeguard and protect the PCD/PII of Plaintiff and Class members from unauthorized disclosure or uses.

116. Additionally, Defendant implicitly promised to retain this PCD/PII only under conditions that kept such information secure and confidential.

117. Plaintiff and Class members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

118. Defendant breached the implied contracts with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff and Class members' PCD/PII, which was compromised as a result of the Data Breach.

119. Defendant further breached the implied contracts with Plaintiff and Class members by otherwise failing to safeguard Plaintiff's and Class members' PCD/PII.

120. Defendant's failures to meet these promises constitute breaches of the implied contracts.

121. Because Defendant allowed unauthorized access to Plaintiff's and Class members' PCD/PII and failed to safeguard the PCD/PII, Defendant breached its contracts with Plaintiff and Class members.

122. A meeting of the minds occurred, as Plaintiff and Class members agreed, *inter alia*, to provide accurate and complete PCD/PII and to pay Defendant in exchange for Defendant's agreement to, *inter alia*, protect their PCD/PII.

123. Defendant breached its contracts by not meeting the minimum level of protection of Plaintiff's and Class members' protected PCD/PII

124. Furthermore, the failure to meet their confidentiality and privacy obligations

resulted in Defendant providing goods and services to Plaintiff and Class members that were of a diminished value.

125. As a direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class members, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PCD/PII is used; (iii) the compromise, publication, and/or theft of their PCD/PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theftand/or unauthorized use of their PCD/PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PCD/PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PCD/PII of customers in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PCD/PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members; and (ix) the diminished value of Defendant's goods and services they received.

126. As a direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class members, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

FOURTH CAUSE OF ACTION
Negligence Per Se
(On Behalf of the Nationwide Class and Florida Subclass)

127. Plaintiff restates and realleges paragraphs 1 through 73 above as if fully set forth herein.

128. 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 Defendant, of failing to use reasonable measures to protect PCD/PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

129. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PCD/PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PCD/PII it obtained and stored, and the foreseeable consequences of a Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiff and Class members.

130. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

131. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

132. The harm that occurred as a result of the 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 members.

133. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity

theft; (ii) the loss of the opportunity how their PCD/PII is used; (iii) the compromise, publication, and/or theft of their PCD/PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PCD/PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PCD/PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PCD/PII of customers in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PCD/PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members; and (ix) the diminished value of Defendant's goods and services they received.

FIFTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of the Nationwide Class and Florida Subclass)

134. Plaintiff restates and realleges paragraphs 1 through 73 above as if fully set forth herein.

135. In light of the special relationship between Defendant and its customers, whereby Defendant became guarantors of Plaintiff's and Class members' highly sensitive, confidential, personal, financial information, and other PCD/PII, Defendant was a fiduciary, created by its undertaking and guarantorship of the PCD/PII, to act primarily for the benefit of their customers, including Plaintiff and Class members, for: 1) the safeguarding of Plaintiff and Class members'

PCD/PII; 2) timely detect a breach and notify Plaintiff and Class members' of a data breach; and 3) maintain complete and accurate records of what and where Defendant's customers' information was and is stored.

136. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of its customer relationship, in particular to keep secure the PCD/PII of its customers.

137. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to diligently investigate the Data Breach to determine the number of Members affected in a reasonable and practicable period of time.

138. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to protect the databases containing Plaintiff's and Class members' PCD/PII.

139. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to timely detect the breach and notify and/or warn Plaintiff and Class members of the Data Breach.

140. Defendant breached its fiduciary duties to Plaintiff and Class members by otherwise failing to safeguard Plaintiff's and Class members' PCD/PII.

141. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PCD/PII is used; (iii) the compromise, publication, and/or theft of their PCD/PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PCD/PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity

theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PCD/PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PCD/PII of customers in its continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PCD/PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members; and (ix) the diminished value of Defendant's goods and services they received.

142. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

SIXTH CAUSE OF ACTION
Breach of Confidence
(On Behalf of the Nationwide Class and Florida Subclass)

143. Plaintiff restates and realleges paragraphs 1 through 73 above as if fully set forth herein.

144. At all times during Plaintiff's and Class members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class members' PCD/PII that Plaintiff and Class members provided to Defendant.

145. As alleged herein and above, Defendant's relationship with Plaintiff and Class members was governed by terms and expectations that Plaintiff's and Class members' PCD/PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

146. Plaintiff and Class members provided their PCD/PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit PCD/PII to be disseminated to any unauthorized parties.

147. Plaintiff and Class members also provided their PCD/PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PCD/PII from unauthorized disclosure, such as following basic principles of information security practices.

148. Defendant voluntarily received in confidence Plaintiff's and Class members' PCD/PII with the understanding that the PCD/PII would not be disclosed or disseminated to the public or any unauthorized third parties.

149. Due to Defendant's failure to prevent, detect, or avoid the Data Breach from occurring by, *inter alia*, following industry standard information security practices to secure Plaintiff's and Class members' PCD/PII, Plaintiff's and Class members' PCD/PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class members' confidence, and without their express permission.

150. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class members have suffered damages.

151. But for Defendant's disclosure of Plaintiff's and Class members' PCD/PII in violation of the parties' understanding of confidence, their protected PCD/PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class members' protected PCD/PII, as well as the resulting damages.

152. The injury and harm Plaintiff and Class members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class members'

PCD/PII.

153. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PCD/PII is used; (iii) the compromise, publication, and/or theft of their PCD/PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theftand/or unauthorized use of their PCD/PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PCD/PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PCD/PII of customers in their continued possession, (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PCD/PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members; and (ix) the diminished value of Defendant's goods and services they received.

154. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

SEVENTH CAUSE OF ACTION
VIOLATION OF FLORIDA'S
DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
Fla. Stat. § 501 *et seq.*
(On Behalf of the Florida Subclass)

155. Plaintiff restates and realleges 1 through 73 above as if fully set forth herein.

156. Plaintiff and the Class Members are "consumers." Fla. Stat. § 501.203(7).

157. Plaintiff and Class Members purchased "things of value" in the form of their goods and services acquired from Defendant. These purchases were made for personal, family, or household purposes. Fla. Stat. § 501.203(9).

158. Defendant engaged in the conduct alleged in this Complaint by advertising and entering into transactions intended to result, and which did result, in the sale of goods or services, to consumers, including Plaintiff and the Class Members. Fla. Stat. § 501.203(8).

159. Defendant engaged in, and its acts and omissions affected trade and commerce. Defendant's acts, practices, and omissions were done in the course of Defendant's business of advertising, marketing, offering to sell, and selling and/or renting goods and services throughout Florida and the United States. Fla. Stat. § 501.203(8).

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

a. Representing that they maintained, but in fact failed to maintain adequate computer systems and data security practices to safeguard Customer Data;

b. representing that their data security practices were adequate, but in fact failed to disclose that their computer systems and data security practices were inadequate to safeguard Customer Data from theft;

c. failure to timely and accurately disclose the Data Breach to Plaintiff and the Class Members;

161. This conduct is considered an unfair method of competition, and constitutes unfair and unconscionable acts and practices. Fla. Stat. § 501.204(1).

162. As a direct and proximate result of Defendant's violation of Florida's Deceptive and Unfair Trade Practices Act ("FDUTPA"), Plaintiff and the Class Members suffered actual damages by paying a premium for Defendant's goods and services with the understanding that at least part of the premium would be applied toward sufficient and adequate information security practices that comply with industry standards, when in fact no portion of that premium was applied toward sufficient and adequate information security practices. Fla. Stat. § 501.211(2).

163. Also, as a direct result of Defendants' knowing violation of FDUTPA, Plaintiff and Class Members are not only entitled to actual damages, but also declaratory judgment that Defendant's actions and practices alleged herein violate FDUTPA, and injunctive relief, including, but not limited to:

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

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures,

d. Ordering that Defendant segment PII by, among other things, creating firewalls and access controls so that if one area of Defendant system is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

f. Ordering that Defendant conduct regular database scanning and securing checks; and

g. Ordering that Defendant routinely and continually conduct 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. Fla. Stat. § 501.211(1).

164. Plaintiff brings this action on behalf of herself and Members of the Florida Sub Class for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff and the Class Members and the public from Defendant's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable, and unlawful practices Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

165. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and the Florida Sub Class Members that they could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

166. Defendant knew or should have known that its data security practices were inadequate to safeguard the Florida Sub Class Members' PCD/PII, and that the risk of a data

disclosure or theft was high.

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

168. Plaintiff and the Florida Sub Class Members seek relief under the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, et seq., including, but not limited to, damages, injunctive relief, and attorneys' fees and costs, and any other just and proper relief.

EIGHTH CAUSE OF ACTION
Violation of Pennsylvania's Unfair Trade Practices and Consumer Protection Law
(On Behalf of the Nationwide Class)

169. Plaintiff restates and realleges paragraphs 1 through 73 above as if fully set forth herein.

170. Plaintiff and the Class Members are "consumers." 73 Pa. S.A. § 201-1.

171. Plaintiff and Class Members purchased things of valuefrom Defendant and through its Website. These purchases were made primarily for personal, family, or household purposes. 73 Pa. S.A. § 201-9.2.

172. Defendant engaged in the conduct alleged in this Complaint by advertising and entering into transactions intended to result, and which did result, in the sale of goods or services, to consumers, including Plaintiff and the Class Members.

173. Defendant engaged in, and its acts and omissions affected trade and commerce. Defendant's acts, practices, and omissions were done in the course of Defendant's business of advertising, marketing, offering to sell, and selling and/or renting goods and services throughout Florida and the United States.

174. Defendant, engaged in deceptive conduct creating a likelihood of confusion or misunderstanding, in violation of 73 Pa. S.A. § 201-3, by:

a. representing (through advertisements and other publication) that it maintained, but in fact failed to maintain adequate computer systems and data security practices to safeguard PCD/PII;

b. representing (through advertisements and other publication) that their data security practices were adequate, but in fact failed to disclose that their computer systems and data security practices were inadequate to safeguard PCD/PII from theft ;

c. failure to timely detect and thus timely disclose the Data Disclosure to Plaintiff and the Class Members;

d. continued acceptance of credit and debit card payments and storage of other PCD/PII after Defendant knew or should have known of the Data Disclosure and before it allegedly remediated the Data Disclosure;

175. This conduct is considered unfair methods of competition, and constitute unfair and deceptive acts and practices. 73 Pa S.A. § 201-2(4).

176. As a direct and proximate result of Defendant's violation of Pennsylvania's Unfair Trade Practices and Consumer Protection Law (UTPCPL), Plaintiff and the Class Members suffered actual damages by paying a premium for Defendant's goods and services with the understanding that at least part of the premium would be applied toward sufficient and adequate information security practices that comply with industry standards, when in fact no portion of that premium was applied toward sufficient and adequate information security practices.

177. Also as a direct result of Defendant's knowing violation of, UTPCPL, Plaintiff and Class Members are not only entitled to actual damages, but also declaratory judgment that

Defendant's actions and practices alleged herein violateUTPCPL , and injunctive relief, including, but not limited to:

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

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment PCD/PII by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy in a reasonable secure manner PCD/PII not necessary for their provisions of services;

f. Ordering that Defendant conduct regular database scanning and securing checks;

g. Ordering that Defendant routinely and continually conduct 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. Ordering Defendant to meaningfully educate 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 Defendant's customers must take to protect themselves.

178. Plaintiff brings this action on behalf of herself and the Class Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff and the Class Members and the public from Defendant's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

179. The above unfair and deceptive practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and the Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

180. Defendant knew or should have known that the lack of encryption on its computer systems and data security practices were inadequate to safeguard the Class Members' PCD/PII and that the risk of a data disclosure or theft was high.

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

182. Plaintiff and the Class Members seek relief under Pennsylvania's Unfair Trade Practices and Consumer Protection Law, 73 Pa. S.A. § 201-1 201-9.2, including, but not limited to, damages, injunctive relief, and attorneys' fees and costs, and any other just and proper relief.

PRAYER FOR RELIEF

WHEREFORE Plaintiff on behalf of herself and all others similarly situated, pray for relief as follows:

a. For an Order certifying the Class as defined herein, and appointing Plaintiff and her

Counsel to represent the Class;

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

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

d. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

e. For an award of punitive damages;

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

g. For prejudgment interest on all amounts awarded; and

h. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

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

Dated: December 31, 2019

Respectfully submitted,

MORGAN & MORGAN
PHILADELPHIA PLLC

BY: */s Kevin Clancy Boylan*
KEVIN CLANCY BOYLAN, ESQ
PA ID. 314117
1800 JFK Blvd., Ste. 1401

Philadelphia PA 19103
P: 215-446-9795
F: 215-446-9799
cboylan@forthepeople.com

MORGAN & MORGAN COMPLEX LITIGATION GROUP
Jean S. Martin (*pro hac vice to be submitted*)
Patrick A. Barthle (*pro hac vice to be submitted*)
Francesca Kester (PA ID 324523, *court admission to be applied for*)
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: (813) 559-4908
Facsimile: (813) 222-4795
jeanmartin@forthepeople.com
pbarthle@forthepeople.com

Attorneys for Plaintiff and the Proposed Class