GEKP

$400

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF PENNSYLVANIA

20 100

DEMETRIUS WILLIAMS, individually and on behalf of all other similarly situated,

Plaintiff,

v.

WAWA, INC.,

Defendant.

Civil Action No. _____

COMPLAINT – CLASS ACTION

JURY TRIAL DEMANDED

FILED
JAN 06 2020
KATE BARKMAN, Clerk
By _____ Dep. Clerk

Plaintiff Demetrius Williams ("Plaintiff"), individually and on behalf of all others similarly situated, allege the following against Defendant Wawa, Inc. ("Wawa" or "Defendant") based on personal knowledge as to his own experience and upon information and belief on investigation of counsel as to all other matters.

INTRODUCTION

Plaintiff brings this action, individually and on behalf of all other similarly situated individuals against Defendant because of Defendant's failure to adequately protect the personal and confidential information of thousands of customers – including credit card and debit card numbers, expiration dates, cardholder names, three or four-digit security codes (commonly referred to as "CVV" codes), and other payment card information (collectively, "Card Information"). This information was compromised in a massive security breach of Wawa's payment processing servers and payment card environment that was publicly disclosed on December 19, 2019 (the "Data Breach"). This Data Breach has harmed Plaintiff and the Class—

consumers who made purchases at Wawa's more than 850 convenience retail stores and gas pumps throughout Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida, and Washington, DC—who have had their sensitive credit and debit Card Information exposed to hackers.

PARTIES

1. Plaintiff Demetrius Williams is an adult residing in Camden, New Jersey.

2. Before the announcement of the Data Breach in December 2019, Plaintiff was a regular customer at several Wawa locations where he purchased goods on numerous occasions between March and December 2019.

3. Like millions of other Wawa customers, Plaintiff used a debit or credit card to make Wawa purchases.

4. Upon information and belief, Plaintiff's Card Information was compromised in the Data Breach.

5. Defendant Wawa, Inc. maintains its headquarters at 260 West Baltimore Pike, Wawa, Pennsylvania 19063.

6. Wawa is a privately-held company founded in 1964 that owns and operates over 850 convenient stores and gas stations located along the east coast in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida, and Washington, D.C. Reports indicate that Wawa stores serve roughly 800 million customers annually.[1]

[1] Maria Aspan, *The Inside Story of Wawa, the Beloved $10 Billion Convenience Store Chain Taking Over the East Coast*, INC. MAGAZINE (June 2018), *available at* https://www.inc.com/magazine/201806/maria-aspan/wawa-convenience-store-pennsylvania.html (last accessed Jan. 3, 2020).

7. With over $10 billion in annual revenue and approximately 35,000 employees,[2] Wawa is one of the largest privately held corporations in the United States. According to Forbes, it ranks as the 25th largest private company in the country in 2019.[3]

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of states different than Wawa. See 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

9. This Court has personal jurisdiction over Wawa, because Wawa has sufficient minimum contacts with the state of Pennsylvania. Wawa maintains its headquarters in the Commonwealth of Pennsylvania and operates numerous Wawa locations and conducts substantial business within this judicial district. Wawa intentionally avails itself of the consumers and markets within the state of Pennsylvania through the promotion, marketing, and sale of its products and services. Thus, this Court has general personal jurisdiction over Wawa. Furthermore, Wawa directs its activities at residents of Pennsylvania on a constant and regular basis by way of, *inter alia*, its operation of hundreds of retail stores in Pennsylvania, and Plaintiff's and Class members' claims arise out of Wawa's operation of retail stores in Pennsylvania; therefore, this Court also has specific personal jurisdiction over Wawa.

---

[2] Wawa, *Our Core Values*, https://www.wawa.com/about (last accessed Jan. 3, 2020).
[3] *America's Largest Private Companies*, FORBES, *available at* https://www.forbes.com/largest-private-companies/list/#tab:rank (last accessed Jan. 3, 2020).

10. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(a)(2) because, as noted above, Wawa conducts substantial business in this district. A substantial part of the events and/or omissions giving rise to the claims occurred within this district.

CASE FACTS

A. Malware and Recent Data Breaches

11. Malware, short for "malicious software," is software designed to infiltrate and damage or destroy computers and computer systems.[4]

12. Malware includes viruses, worms, Trojan horse viruses, spyware, adware, and ransomware.[5]

13. One specific type of malware is point-of-sale (POS) malware. POS malware is used "to steal information related to financial transactions, including credit card information."[6]

14. It is well known in the retail industry that sensitive Card Information is valuable and frequently targeted by hackers. In a recent article, Business Insider noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers …. Many of them were caused by flaws in payment systems either online or in stores."[7]

---

[4] *What is Malware?*, Cisco Worldwide, *available at* https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html (last accessed Jan. 3, 2020).
[5] *Id.*
[6] *PoS (Point-of-Sale) Malware*, Trend Micro, *available at* https://www.trendmicro.com/vinfo/us/security/definition/pos-(point-of-sale)-malware (last accessed Jan. 3, 2020).
[7] Dennis Green et al., *If you bought anything from these 11 companies in the last year, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019), *available at* https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1 (last accessed Jan. 3, 2020).

15. Malware has been used recently to infiltrate large retailers such as, *inter alia*, Checkers,[8] Target, HomeDepot,[9] GameStop,[10] Chipotle, Wendy's, Whole Foods,[11] Sally Beauty,[12] and Michaels Stores.[13]

16. One commentator in the data security industry noted as to a previous, unrelated data breach:

> POS-malware breaches happen in the US with alarming regularity, and businesses should be well aware that they need to not only protect their central networks but also need to account for physical locations as well. Moving forward, financial institutions should consider implementing a system of two-factor authentication in conjunction with a passive biometric solutions in order to mitigate the entirely avoidable outcomes of security incidents such as this.[14]

17. Despite the known risk of POS malware intrusions and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Wawa failed to take reasonable steps to adequately protect its computer systems and payment card environment from being breached, and then failed to detect the Data Breach for many months.

---

[8] Bradley Barth, *POS malware swipes payment info from Checkers and Rally's restaurants*, SC Magazine (May 30, 2019), *available at* https://www.scmagazine.com/home/security-news/cybercrime/pos-malware-swipes-payment-info-from-checkers-and-rallys-restaurants/ (last accessed Jan. 3, 2020).

[9] Taylor Armerding, *The 18 biggest data breaches of the 21st century*, CSO MAGAZINE (Dec. 20, 2018), *available at* https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (last accessed Jan. 3, 2020).

[10] Ian Paul, *Lengthy GameStop hack may have compromised customer credit cards, personal info*, PC World (Apr. 10, 2017), *available at* https://www.pcworld.com/article/3188558/lengthy-gamestop-hack-may-have-compromised-customer-credit-cards-personal-info.html (last accessed Jan. 3, 2020).

[11] Jackie Wattles, *The list grows: Whole Foods hit by hackers*, CNN BUSINESS (Sept. 28, 2017), *available at* https://money.cnn.com/2017/09/28/technology/business/whole-foods-data-breach/index.html (last accessed Jan. 3, 2020).

[12] Josh Beckerman, *Sally Beauty Says Malware Used at Some Point-of-Sale Systems in March and April*, WALL ST. J. (May 28, 2015), *available at* https://www.wsj.com/articles/sally-beauty-says-malware-used-at-some-point-of-sale-systems-in-march-and-april-1432858599 (last accessed Jan. 3, 2020).

[13] Elizabeth A. Harris, *Michaels Stores' Breach Involved 3 Million Customers*, N.Y. TIMES (Apr. 19, 2014), *available at* https://www.nytimes.com/2014/04/19/business/michaels-stores-confirms-breach-involving-three-million-customers.html (last accessed Jan. 3, 2020).

[14] *Cyber Attack on Earl Enterprises (Planet Hollywood)*, ISBUZZNEWS (Apr. 1, 2019), *available at* https://www.informationsecuritybuzz.com/expert-comments/cyber-attack-on-earl-enterprises-planet-hollywood/ (last accessed Jan. 3, 2020).

B. Wawa Data Breach

18. Wawa's professed Core Values include "valu[ing] people," "do[ing] the right thing," and "do[ing] things right."[15] However, Wawa has failed to uphold these values in both its data security measures and how it has handled the data breach.

19. On December 19, 2019, several media outlets reported that Wawa had experienced a data breach that compromised its payment systems.[16]

20. That day, Wawa posted "An Open Letter from Wawa CEO Chris Gheysens to Our Customers" ("Open Letter") on its website, which indicated that it had been made aware of a malware intrusion on Wawa's payment processing servers that compromised its payment card environment and customers' sensitive Card Information. The Open Letter provides the following, in pertinent part:

> Dear Wawa Customers,
>
> 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.[17]

21. As confirmed by the Open Letter, Wawa believes the Data Breach occurred sometime on or after March 4, 2019. But Wawa did not discover it until December 10, 2019, leaving customers' sensitive information exposed to criminals for nearly nine months.

---

[15] Wawa, *Our Core Values*, https://www.wawa.com/about (last accessed Jan. 3, 2020).
[16] *See, e.g.,* Isabel Hughes, *Wawa warns of 'data security incident' involving credit and debit card information,* USA TODAY (Dec. 19, 2019), *available at* https://www.usatoday.com/story/money/2019/12/19/wawa-data-breach-2019-company-warns-data-security-incident/2703276001/ (last accessed Jan. 3, 2020).
[17] Wawa, *Open Letter from Wawa CEO Chris Gheysens to Our Customers* (Dec. 19, 2019), *available at* https://www.wawa.com/alerts/data-security (last accessed Jan. 3, 2020).

22. The Open Letter also revealed that, while there were different timeframes for the Data Breach at Wawa's different locations, the malware affected most of its store systems. The Open Letter states:

> Based on our investigation to date, we understand that at different points in time after March 4, 2019, malware began running on in-store payment processing systems at potentially all Wawa locations. Although the dates may vary and some Wawa locations may not have been affected at all, this malware was present on most store systems by approximately April 22, 2019. Our information security team identified this malware on December 10, 2019, and by December 12, 2019, they had blocked and contained this malware.[18]

23. In addition to the Open Letter, Wawa's website contains a link to "FAQs" regarding the data breach, which explain that in addition to in-store payment terminals and fuel dispensers, Wawa gift cards may also have been affected by the malware.[19]

24. Wawa also issued a Press Release,[20] notifying customers of the data security incident:

---

[18] *Id.* (emphasis added).
[19] *See* FAQs (Dec. 19, 2019), *available at* https://www.wawa.com/alerts/data-security (last accessed Jan. 3, 2020).
[20] *See* Press Release: *Wawa Notifies Customers of Data Security Incident* (Dec. 19, 2019), *available at* https://s3.amazonaws.com/wawa-kentico-prod/wawa/media/misc/wawa-data-security-incident-wire-release-12_19_2019.pdf (last accessed Jan. 3, 2020).

Contact: public.relations@wawa.com

Wawa Notifies Customers of Data Security Incident

Wawa, PA (December 19, 2019) – Wawa is notifying potentially impacted individuals about a data security incident that affected customer payment card information used at potentially all Wawa locations during a specific timeframe. Based on the investigation to date, the information is limited to payment card information, including debit and credit card numbers, expiration dates and cardholder names, but does not include PIN numbers or CVV2 numbers. The ATM cash machines in Wawa stores were not impacted by this incident. At this time, Wawa is not aware of any unauthorized use of any payment card information as a result of this incident.

Wawa's information security team discovered malware on Wawa payment processing servers on December 10, 2019, and contained it by December 12, 2019. After discovering this malware, Wawa immediately engaged a leading external forensics firm and notified law enforcement. Based on Wawa's forensic investigation, Wawa now understands that this malware began running at different points in time after March 4, 2019. Wawa took immediate steps after discovering this malware and believes it no longer poses a risk to customers.

"At Wawa, the people who come through our doors are not just customers, they are our friends and neighbors, and nothing is more important than honoring and protecting their trust," said Chris Gheysens, Wawa CEO. "Once we discovered this malware, we immediately took steps to contain it and launched a forensics investigation so that we could share meaningful information with our customers. I want to reassure anyone impacted they will not be responsible for fraudulent charges related to this incident. To all our friends and neighbors, I apologize deeply for this incident."

Wawa is supporting its customers by offering identity protection and credit monitoring services at no charge to them. Information about how to enroll can be found on the Wawa website below. Wawa has also established resources to answer customers' questions, including a dedicated call center that can be reached at 1-844-386-9559, Monday - Friday, between 9:00 am and 9:00 pm Eastern Time or Saturday and Sunday between 11:00 am and 8:00 pm, excluding holidays. Wawa has also posted information on its website, www.wawa.com, including a letter from Wawa's CEO and more details for impacted customers.

A detailed notice and open letter to customers from Wawa's CEO notifying potentially affected individuals about the incident is available at www.wawa.com/alerts/data-security

ABOUT WAWA
Wawa, Inc. is a chain of convenience and fuel retail stores located in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Washington, DC and Florida.

###

25. However, neither the Open Letter, Press Release, nor any public statements issued by Wawa give any indication as to the actual magnitude of the Data Breach, including confirmation of the exact number of stores impacted or the actual number of customers and cards affected. Upon information and belief, Wawa has not taken any steps to notify potentially impacted customer beyond the Open Letter and Press Release.

26. Wawa has not disclosed how many customers have been affected by the breach. However, it is "highly likely" that customers who used credit or debit cards at Wawa locations between March 4 and December 12, 2019 could have had their data compromised.[21]

27. Although the Open Letter indicates Wawa also "notified law enforcement and payment card companies, and engaged a leading external forensics firm to support our response efforts,"[22] it is still unclear what such efforts involve, as Wawa has not disclosed exactly what was communicated to authorities.

C. Standards for Protecting Card Information

28. Wawa is, and at all relevant times has been, aware that the Card Information it maintains as a result of purchases made at its locations is highly sensitive and could be used for nefarious purposes by third parties.

29. Wawa's explicit statements in its Privacy Policy make clear that Wawa recognized the importance of adequately safeguarding its customers' sensitive Card Information, yet Wawa failed to take the steps necessary to protect that sensitive data. On its website, Wawa's Privacy Policy provides the following:

---

[21] Sophia Waterfield, *Wawa Data Breach 2019: How to Check if You Have Been Affected*, NEWSWEEK (Dec. 20, 2019), *available at* https://www.newsweek.com/wawa-data-breach-2019-how-check-if-you-have-been-affected-1478437 (last accessed Jan. 3, 2020).

[22] *Id.*

Wawa Official Privacy Policy

> Protecting your privacy is important to Wawa. This Wawa Privacy Policy ('Policy') describes how Wawa and its subsidiaries and affiliated companies collect, use, disclose and safeguard the personal information you provide on Wawa's websites, www.wawa.com and www.wawarewards.com, and through or in connection with our mobile apps or other software- and Internet-enabled programs and services sponsored by Wawa (the "Sites") as well as information collected when you visit our stores or otherwise communicate or interact with Wawa.[23]

30. The Privacy Policy goes on to explain the types of information collected and how Wawa may use such information.

31. Wawa is thus aware of the importance of safeguarding its customers' Card Information from the foreseeable consequences that would occur if its data security systems and computer servers were breached.

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

33. The Payment Card Industry Data Security Standard ("PCI DSS") is a list of twelve information security requirements that were promulgated by the Payment Card Industry Security Standards Council. The PCI DSS list applies to all organizations and environments where cardholder data is stored, processed, or transmitted, and requires merchants like Wawa to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies.

[23] *See* Wawa Official Privacy Policy, Effective Date May 2019, *available at* https://www.wawa.com/privacy (last accessed Jan. 3, 2020).

34. The twelve requirements of the PCI DSS are: (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; (3) Protect stored cardholder data; (4) Encrypt transmission of cardholder data across open, public networks; (5) Protect all systems against malware and regularly update anti-virus software or programs; (6) Develop and maintain secure systems and applications; (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; (10) Track and monitor all access to network resources and cardholder data; (11) Regularly test security systems and processes; (12) Maintain a policy that addresses information security for all personnel.[24]

35. Furthermore, PCI DSS sets forth detailed and comprehensive requirements that must be followed to meet each of the twelve mandates.

36. Given its participation in payment card processing networks and the daily collection and transmission of thousands of sets of Card Information, Wawa was, at all material times, fully aware of its data protection obligations.

37. Because Wawa accepted payment cards containing sensitive financial information, it knew that its customers were entitled to and did in fact rely on it to keep that sensitive information secure from would-be data thieves in accordance with the PCI DSS requirements.

38. Additionally, according to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to

[24] PCI SECURITY STANDARDS COUNCIL, *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard Version 3.2*, at 9 (May 2016), *available at* https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf?agreement=true&time (last accessed Jan. 3, 2020).

confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45.

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

40. The FTC has also published a document, entitled "Protecting Personal Information: A Guide for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[25]

41. The FTC has issued orders against businesses that failed to employ reasonable measures to secure payment card data. These orders provide further guidance to businesses with regard to their data security obligations.

[25] FEDERAL TRADE COMMISSION, *Protecting Personal Information: A Guide for Business* (Nov. 2011), *available at* https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed Jan. 3, 2020).

D. Standards for Customer Data Security

42. As noted above, Wawa should have been and, based upon its acknowledged use of encryption technology at certain locations, was aware of the need to have adequate data security systems in place.

43. Despite this, Wawa failed to upgrade and maintain its data security systems in a meaningful way in order prevent data breaches. Wawa's security flaws run afoul of industry best practices and standards. More specifically, the security practices in place at Wawa are in stark contrast and directly conflict with the PCI DSS core security standards.

44. Had Wawa properly maintained its information technology systems ("IT systems"), adequately protected them, and had adequate security safeguards in place, it could have prevented the Data Breach and/or could have promptly detected the Data Breach when it occurred.

45. As a result of industry warnings, awareness of industry best practices, the PCI DSS, and numerous well-documented restaurant and retail (and other) data breaches, Wawa was alerted to the risk associated with failing to ensure that its IT systems were adequately secured.

46. Wawa was not only aware of the threat of data breaches, generally, but was aware of the specific danger of malware infiltration. As a result, Wawa was aware that malware is a real threat and is a primary tool of infiltration used by hackers seeking to carry out payment card breaches.

47. In addition to the publicly announced data breaches described above (among many others), Wawa knew or should have known of additional warnings regarding malware infiltrations from the U.S. Computer Emergency Readiness Team, a government unit within the Department of Homeland Security, which alerted retailers to the threat of malware on July 31,

2014, and issued a guide for retailers on protecting against the threat of malware, which was updated on August 27, 2014.[26]

48. Despite the fact that Wawa was on notice of the very real possibility of consumer data theft associated with its security practices and that Wawa knew or should have known about the elementary infirmities associated with its security systems, it still failed to make necessary changes to its security practices and protocols, and permitted the Data Breach to continue for approximately nine months.

49. Wawa, at all times relevant to this action, had a duty to Plaintiff and members of the Class to: (a) properly secure Card Information submitted to or collected at Wawa's locations and on Wawa's internal networks; (b) encrypt Card Information using industry standard methods; (c) use available technology to defend its systems from known methods of invasion; (d) act reasonably to prevent the foreseeable harms to Plaintiff and Class members, which would naturally result from Card Information theft; and (e) promptly notify customers when Wawa became aware that customers' Card Information may have been compromised.

50. Wawa permitted customers' Card Information to be compromised by failing to take reasonable steps against a known threat.

51. In addition, leading up to the Data Breach, during the breach itself, and during the investigation that followed, Wawa failed to follow the guidelines set forth by the FTC.

52. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has identified that: "If your data

[26] *See* U.S. COMPUTER EMERGENCY READINESS TEAM, *Alert (TA14-212A): Backoff Point-of-Sale Malware* (July 31, 2014) (revised Sept. 30, 2016), *available at* https://www.us-cert.gov/ncas/alerts/TA14-212A (last accessed Jan. 3, 2020).

was stolen through a data breach that means you were somewhere out of compliance" with payment industry data security standards.[27]

53. The Data Breach is particularly egregious and Wawa's data security failures are particularly alarming given that the breach went undetected for so long, exposing millions of customers' sensitive data to criminals for nearly nine months. Clearly, had Wawa utilized adequate data security and data breach precautions, the window of the Data Breach would have been significantly mitigated, and the level of impact significantly reduced (had the breach been permitted to occur at all).

54. With more than 850 Wawa locations potentially affected, and likely millions of sets of Card Information stolen, this clearly marks a highly successful outing for criminals and a large failure on Wawa's part as to data security.

55. Because payment card data breaches involving malware are so common, and given the high level of data security measures available to companies that take customer payment information in, like Wawa, there is no reason why Wawa could not have adequately protected its systems and servers from the Data Breach.

56. As a result of the Data Breach, Plaintiff and Class members suffered actual fraud and losses resulting from the Data Breach, including: financial losses related to the purchases made at Wawa that Plaintiff and Class members would not have made had they known of Wawa's negligent approach to cybersecurity; lost control of Card Data; unreimbursed losses relating to fraudulent charges; losses and fees relating to exceeding credit and debit card limits, balances, and bounced transactions; harm resulting from damaged credit scores and information; loss of time and money resolving fraudulent charges; loss of time and money monitoring

[27] Lisa Baertlin, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017), *available at* https://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY (last accessed Jan. 3, 2020).

accounts for fraudulent transactions, loss of time and money obtaining protections against future identity theft; loss of rewards points or airline mileage available on credit cards that consumers lost credit for as a result of having to use alternative forms of payment while awaiting replacement cards; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information.

57. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges occur and are discovered.

58. Furthermore, the Card Information stolen from Wawa's locations can be used to drain debit card-linked bank accounts or to buy items on certain less-secure websites.

59. Wawa customers' stolen Card Information may also be sold on the "dark web" at some undetermined point in the future. In March 2018, a hacking group announced the sale of over 5 million stolen payment cards.[28] A year later, over 2 million stolen payment cards were sold on the dark web.[29] After criminals buy this stolen information, they can use it to "clone" counterfeit cards.

60. Recognizing the repercussions from its wrongful actions and inactions and the resulting Data Breach, Wawa claims it is now offering credit monitoring and identity protection at the credit monitoring bureau of its choice. However, this belated remedy does nothing to protect against the millions of customers who had their sensitive data exposed to criminals for nearly nine months, and does not ensure protection from fraud going forward. Furthermore, upon information and belief, to date Wawa has not offered to reimburse customers who have already

[28] *Bank Card Data of Five Million Stolen in Sakes and Lord & Taylor Data Breach*, Trend Micro, *available at* https://www.trendmicro.com/vinfo/my/security/news/cybercrime-and-digital-threats/-bank-card-data-of-five-million-stolen-in-saks-and-lord-taylor-data-breach (last accessed Jan. 3, 2020).

[29] Lisa Vaas, *2m credit cards ripped off from restaurant chain sold on the dark web*, Naked Security (Apr, 3, 2019), *available at* https://nakedsecurity.sophos.com/2019/04/03/2m-credit-cards-ripped-off-from-restaurant-chain-sold-on-the-dark-web/ (last accessed Jan. 3, 2020).

paid for their own fraud protection or credit monitoring services after learning of the data breach on or after December 12, 2019.

61. Wawa's failure to adequately protect its customers' Card Information has resulted in consumers having to undertake various tasks (e.g., obtaining credit monitoring, checking credit reports, monitoring accounts, etc.) that require time and effort and, for many of the credit and fraud protection services, payment of their own money. At the same time, Wawa is doing nothing to assist those affected by the Data Breach and has withheld important details about the Data Breach as it conducts its investigation. Instead, Wawa is putting the burden on the consumer to discover possible fraudulent transactions.

CLASS ALLEGATIONS

62. Plaintiff brings this action individually and on behalf of the following class ("the Class") pursuant to Fed. R. Civ. P. 23:

> All persons who had their credit or debit card information compromised as a result of the Wawa Data Breach.

63. Excluded from the Class are Wawa, its affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change, or expand the definitions of the Class based on discovery and further investigation.

64. **Numerosity:** While the precise number of Class members has not yet been determined, members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class includes many geographically dispersed Class members. Upon information and belief, the Data Breach affected thousands, if not millions, of Wawa customers across the United States.

65. **Typicality:** Plaintiff's claims are typical of Class members' claims. Plaintiff and all Class members were injured through Wawa's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each Class member had their sensitive data and Card Information compromised in the same way by the same conduct by Wawa.

66. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class that they seek to represent; Plaintiff has retained counsel that are competent and highly experienced in class action litigation, including data breach cases in particular; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

67. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class members. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class members individually to effectively redress Wawa's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

68. **Common Questions of Fact and Law:** Common questions of law and fact exist as to Plaintiff and all class members. These questions predominate over the questions affecting individual class members. These common legal and factual questions include, but are not limited to, the following:

a. whether Wawa engaged in the wrongful conduct alleged herein;

b. whether Wawa owed duties to Plaintiff and members of the class to protect their Card Information and to provide timely and accurate notice of the Data Breach to Plaintiff and the class, and whether it breached these duties;

c. whether Wawa violated federal and state laws as a result of the Data Breach;

d. whether Wawa knew or should have known that its computer and network systems were vulnerable to attacks from hackers and cyber-criminals;

e. whether Wawa's conduct was the proximate cause of the breach of its computer and network systems resulting in the theft of customers' Card Information;

f. whether Wawa wrongfully failed to inform Plaintiff and members of the class that it did not maintain computer software and other security procedures and precautions sufficient to reasonably safeguard consumers' sensitive financial and personal data;

g. whether Wawa failed to inform Plaintiff and the class of the Data Breach in a timely and accurate manner;

h. whether Wawa has taken adequate preventive and precautionary measures to ensure Plaintiff and class members will not experience further harm;

i. whether Wawa violated the New Jersey Consumer Fraud Act;

j. whether Plaintiff and members of the class suffered injury as a proximate result of Wawa's conduct or failure to act; and

k. whether Plaintiff and the class are entitled to recover damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiff and the class.

69. Wawa has acted or refused to act on grounds generally applicable to Plaintiff and the other members of the Class, thereby making appropriate final injunctive relief and declaratory relief with respect to the Class as a whole.

70. Given that Wawa has engaged in a common course of conduct as to Plaintiff and the Class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

71. The Class is defined in terms of objective characteristics and common transactional facts; namely, the exposure of sensitive Card Information to cyber criminals due to Wawa's failure to protect this information, adequately warn the Class that it lacked adequate data security measures, and failure to adequately warn that it was breached. Class membership will be readily ascertainable from Wawa's business records, and/or from records of third parties.

72. Plaintiff reserves the right to revise the above Class definitions and any of the averments of fact herein based on facts adduced in discovery.

COUNT I

NEGLIGENCE

(On Behalf of Plaintiff and the Class)

73. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

74. Wawa collected Card Information from Plaintiff and Class members in exchange for its sale of food and other services at its impacted locations.

75. Wawa owed a duty to Plaintiff and the Class to maintain confidentiality and to exercise reasonable care in safeguarding and protecting their financial and personal information in Wawa's possession from being compromised by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Wawa's networks and data security

systems to ensure that Plaintiff's and Class members' financial and personal information in Wawa's possession was adequately protected in the process of collection and following collection while stored on Wawa's systems.

76. Wawa further owed a duty to Plaintiff and Class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

77. Wawa owed a duty to Plaintiff and Class members to provide security consistent with industry standards and requirements and to ensure that its computer systems and networks— and the personnel responsible for them—adequately protected the financial and personal information of Plaintiff and Class members whose confidential data Wawa obtained and maintained.

78. Wawa knew, or should have known, of the risks inherent in collecting and storing Plaintiff's and Class members' financial and personal information and the critical importance of providing adequate security for that information.

79. Wawa's conduct created a foreseeable risk of harm to Plaintiff and Class members. This conduct included but was not limited to Wawa's failure to take the steps and opportunities to prevent and stop the Data Breach as described herein. Wawa's conduct also included its decision not to comply with industry standards for the safekeeping and maintenance of the financial and personal information of Plaintiff and Class members.

80. Wawa knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and Wawa knew or should have known that hackers would attempt or were attempting to access the personal financial information in databases such as Wawa's.

81. Wawa breached the duties it owed to Plaintiff and members of the Class by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the medical, financial, and personal information of Plaintiff and members of the Class, as identified above. This breach was a proximate cause of injuries and damages suffered by Plaintiff and Class members.

82. As a direct and proximate result of Wawa's negligent conduct, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial.

COUNT II

NEGLIGENCE *PER SE*

(On Behalf of Plaintiff and the Class)

83. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

84. Pursuant to the FTC Act, 15 U.S.C. § 45, Wawa had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class members' personal information.

85. 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 Card Information. The FTC publications and orders described above also form part of the basis of Wawa's duty to protect Plaintiff's and Class members' sensitive information.

86. Wawa violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Card Information and not complying with applicable industry standards, including PCI DSS, as described in detail herein. Wawa's conduct was particularly unreasonable given the nature and amount of Card Information it collected and stored and the

foreseeable consequences of a data breach, including, specifically, the immense damages that would result to consumers and financial institutions.

87. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, 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.

88. Wawa had a duty to Plaintiff and Class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class members' personal information.

89. Wawa breached its duties to Plaintiff and Class members under the FTC Act (and similar state statutes), by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' financial and personal information.

90. Wawa's violation of Section 5 of the FTC Act (and similar state statutes) and its failure to comply with applicable laws and regulations constitutes negligence per se.

91. But for Wawa's wrongful and negligent breach of its duties owed to Plaintiff and Class members, they would not have been injured.

92. The injury and harm suffered by Plaintiff and Class members was the reasonably foreseeable result of Wawa's breach of its duties. Wawa knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and Class members to suffer the foreseeable harms associated with the exposure of their Card Information.

93. Had Plaintiff and Class members known that Wawa did and does not adequately protect customer Card Information, they would not have made purchases at Wawa's locations.

94. As a direct and proximate result of Wawa's negligence per se, Plaintiff and Class members have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Wawa that Plaintiff and Class members would not have made had they known of Wawa's careless approach to cyber security; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information, entitling them to damages in an amount to be proven at trial.

COUNT III

BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiff and the Class)

95. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

96. Plaintiff and Class members who made purchases at Wawa's locations during the period in which the Data Breach occurred had implied contracts with Wawa.

97. Specifically, Plaintiff and Class members paid money to Wawa and, in connection with those transactions, provided Wawa with their Card Information. In exchange, Wawa agreed, among other things: (1) to provide food, gasoline, and food services to Plaintiff and Class members at its various locations; (2) to take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' Card Information; and (3) to protect Plaintiff's

and Class members' personal information in compliance with federal and state laws and regulations and industry standards.

98. Protection of personal information is a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Wawa, on the other hand. Indeed, as set forth, supra, Wawa recognized the importance of data security and privacy of customers' sensitive financial information in the privacy policy. Had Plaintiff and Class members known that Wawa would not adequately protect customer Card Information, they would not have made purchases at Wawa's locations.

99. Wawa did not satisfy its promises and obligations to Plaintiff and Class members under the implied contracts because it did not take reasonable measures to keep their personal information secure and confidential and did not comply with the applicable laws, regulations, and industry standards.

100. Wawa materially breached its implied contracts with Plaintiff and Class members by failing to implement adequate payment card and Card Information security measures.

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

102. Wawa's failure to satisfy its obligations led directly to the successful intrusion of Wawa's computer servers and stored Card Information and led directly to unauthorized parties' access and exfiltration of Plaintiff's and Class members' Card Information.

103. Wawa breached these implied contracts as a result of its failure to implement security measures.

104. Also, as a result of Wawa's failure to implement the security measures, Plaintiff and Class members have suffered actual damages resulting from the theft of their personal information and remain at imminent risk of suffering additional damages in the future.

105. Accordingly, Plaintiff and Class members have been injured as a proximate result of Wawa's breaches of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV

BREACH OF CONTRACTS TO WHICH PLAINTIFF AND CLASS MEMBERS WERE INTENDED THIRD-PARTY BENEFICIARIES

(On Behalf of Plaintiff and the Class)

106. Plaintiff realleges and incorporates all foregoing substantive allegations as if fully set forth herein.

107. Upon information and belief, Plaintiff and Class members are intended third-party beneficiaries of contracts entered into between Wawa and various entities including, without limitation, (i) contracts between Wawa and its customers to process credit card and/or debit card transactions, (ii) contracts between Wawa and Visa and/or MasterCard (including their operating regulations), and (iii) contracts between Wawa and the acquiring banks that accept and process payment card transactions at Wawa's locations.

108. Upon further information and belief, these contracts and regulations require, inter alia, that Wawa take appropriate steps to safeguard the sensitive financial information of Wawa's customers, like Plaintiff and Class members.

109. Plaintiff and the Class members are intended third party beneficiaries of these contracts and regulations. Under the circumstances, recognition of a right to performance is appropriate to effectuate the intentions of the parties to these contracts. One or more of the

parties to these contracts intended to give Plaintiff and the Class members the benefit of the performance promised in the contracts.

110. Wawa breached these agreements, which directly and/or proximately caused Plaintiff and the Class members to suffer substantial damages.

111. Upon further information and belief, Wawa saved (or avoided spending) a substantial sum of money by knowingly failing to comply with its contractual obligations and continues to do so.

112. Accordingly, Plaintiff and Class members who have been injured are entitled to damages, restitution, and other relief in an amount to be proven at trial.

COUNT V

VIOLATION OF THE NEW JERSEY CONSUMER FRAUD ACT, N.J. STAT. ANN. § 56:8-2, *et seq.*

(On Behalf of Plaintiff and the Class)

113. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

114. Plaintiff and Class members are consumers who used their credit or debit cards to purchase convenient store items and gasoline products for personal, family and household purposes from Wawa locations in New Jersey.

115. Wawa engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of "merchandise" to consumers, as defined by N.J. STAT. ANN. § 56:8-1.

116. Wawa is engaged in, and its acts and omissions affect, trade and commerce. 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.

117. The New Jersey Consumer Fraud Act ("NJCFA"), N.J. STAT. ANN. § 56:8-2, *et seq.*, 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.

118. 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 members of the Class.

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

120. 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 the security vulnerability, and members of the Class could not reasonably be expected to learn or discover the true facts.

121. As alleged herein, Wawa engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and the sale of food products, gasoline products, goods or services to consumers in the state of New Jersey, in violation of the NJCFA, including but not limited to:

a. Failing to adequate secure the sensitive financial information of members of the Class;

b. Failing to maintain adequate computer systems and data security practices to safeguard customers' personal and financial information;

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. Misrepresenting the material fact that Wawa did and would comply with the requirements of relevant federal and state laws and industry standards pertaining to the privacy and security of the sensitive financial information of members of the Class;

e. 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;

f. Failing to disclose in a timely and accurate manner to the Class the material fact of the nature and extent of the Data Breach; and

g. Continuing to accept credit and debit card payments and storage of other personal information after Wawa knew or should have known of the data breach and before it allegedly remedied the breach.

122. By engaging in the conduct alleged above, Wawa has violated the NJCFA by, inter alia:

a. Omitting material facts regarding the goods and services sold;

b. Omitting material facts regarding the financial transactions, particularly the security thereof, between Wawa and its customers for the purchase of food products, gasoline, goods and services;

c. Misrepresenting material facts in the furnishing or sale of food products, gasoline, goods and services;

d. Engaging in conduct that is likely to mislead consumers acting reasonably under the circumstances;

e. Engaging in conduct which creates a likelihood of confusion or of misunderstanding;

f. Engaging in conduct that is immoral, unethical, oppressive and unscrupulous;

g. Unfair practices that caused or were likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers; and/or

h. Other unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices to be shown at trial.

123. Wawa's actions engaging in the conduct above were negligent, knowing and willful and/or wanton and reckless with respect to the rights of the Class.

124. As a direct and proximate result of Wawa's violation of the NJCFA, members of the Class have suffered ascertainable losses of moneys and actual damages including, inter alia:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their personal and financial information by criminals;

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

d. costs associated with the unauthorized use of their financial accounts;

e. loss and 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;

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

g. impending injury flowing from potential fraud and identity theft posed by their credit card and personal information being placed in the hands of criminals and already being misused;

h. impairment to their credit scores and ability to borrow and/or obtain credit; 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.

125. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of Wawa alleged herein, the Class 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.

126. Pursuant to N.J. STAT. ANN. § 56:8-20, this Complaint will be served upon the New Jersey Attorney General.

COUNT VI

VIOLATION OF THE NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT, N.J. STAT. ANN. §§ 56:8-163 *et seq.*

(On Behalf of Plaintiff and the Class)

127. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

128. Wawa is a business that conducts business in New Jersey under N.J. STAT. ANN. § 56:8-163(a).

129. Plaintiff's and Class members' Card Information includes personal information as defined in N.J. STAT. ANN. §§ 56:8-163 *et seq.*

130. Under N.J. STAT. ANN. § 56:8-163(a), "[a]ny business that conducts business in New Jersey…shall disclose any breach of security of [] computerized records following discovery or notification of the breach to any customers who is a resident of New Jersey whose personal information was, *or is reasonably believed to have been*, accessed by an unauthorized person." (emphasis added).

131. Because Wawa discovered a breach of its security system involving the Card Information of Plaintiff and Class members, in which such Card Information was, or is reasonably believed to have been, acquired by an unauthorized person, and the Card Information

was not secured. Wawa had an obligation to disclose the breach in a timely and accurate fashion under N.J. STAT. ANN. § 56:8-163 *et seq.*

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

133. As a direct and proximately result of this violation, Plaintiff and Class members suffered the damages described above.

134. Plaintiff and Class members seek relief under N.J. Stat. Ann. § 56:8-19, including treble damages, attorneys' fees and costs, and injunctive relief.

COUNT VII

UNJUST ENRICHMENT

(On Behalf of Plaintiff and the Class)

135. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

136. This claim is plead in the alternative to the above implied contract claim.

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

138. Wawa appreciated or had knowledge of the benefits conferred upon them by Plaintiff and Class members. Wawa also benefited from the receipt of Plaintiff's and Class members' Card Information, as this was utilized by Wawa to facilitate payment to it.

139. The monies Plaintiff and Class members paid to Wawa were supposed to be used by Wawa, in part, to pay for adequate data privacy infrastructure, practices, and procedures.

140. As a result of Wawa's conduct, Plaintiff and Class members 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 members

paid for, and those purchases without adequate data privacy and security practices and procedures that they received.

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

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

PRAYER FOR RELIEF

Plaintiff, on behalf of himself and the Class, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23(a) and (b), and, pursuant to Fed. R. Civ. P. 23(g), appoint Plaintiff as Class representative and his counsel as Class counsel.

B. Award Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement.

C. Award Plaintiff and the Class equitable, injunctive, and declaratory relief as may be appropriate. Plaintiff, on behalf of the Class, seeks appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing best security data practices to safeguard customers' financial and personal information, extend credit monitoring services and similar services to protect against all types of identity

theft, including card theft and fraudulent card charges, and to provide elevated credit monitoring services to minor and elderly Class members who are more susceptible to fraud and identity theft.

D. Award Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable.

E. Award Plaintiff and the Class reasonable attorneys' fees and costs as allowable.

F. Award Plaintiff and the Class such other favorable relief as allowable under law or at equity.

Dated: January 6, 2020

Respectfully submitted,

/s/ Eugene A. Spector

Eugene A. Spector
John A. Macoretta
Diana J. Zinser
SPECTOR ROSEMAN & KODROFF, P.C.
2001 Market Street, Suite 3420
Philadelphia, PA 19103
Phone: (215) 496-0300
Fax: (215) 496-6611
espector@srkattorneys.com
jmacoretta@srkattorneys.com
dzinser@srkattorneys.com

David P. McLafferty
MCLAFFERTY LAW FIRM, P.C.
923 Fayette Street
Conshohocken, PA 19428
Phone: (610) 940-4000 ext. 12
dmclafferty@mclaffertylaw.com

Attorneys for Plaintiff and the Proposed Class

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on this 6th day of January 2020, a true and correct copy of the above and foregoing was filed with the Clerk of Court via the Court's CM/ECF system for electronic service on all counsel of record and counsel in related actions below and mailed via certified mail to Wawa, Inc. located at Red Roof, 260 Baltimore Pike, Wawa, Pennsylvania 19063:

Case Name	Case No.	Counsel	Counsel
Rapak v. Wawa, Inc.	2:19-cv-06019	Anthony M. Christina (PA ID# 322528) **LOWEY DANNENBERG,** One Tower Bridge 100 Front Street, Suite 520 West Conshohocken, PA 19428 Telephone: (215) 399-4770 Email: achristina@lowery.com	Vincent Briganti *(pro hac vice* forthcoming) Christian Levis *(pro hac vice* forthcoming) **LOWEY DANNENBERG, P.C.** 44 South Broadway, Suite 1100 White Plains, NY 10601 Telephone: (914) 997-0500 Email: vbriganti@lowery.com clevis@lowery.com jseredynski@lowery.com
Kaufman v. Wawa, Inc.	2:19-cv-06032	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	Melissa R. Emert **STULL, STULL & BRODY** 6 East 45th St., 5th Floor New York, NY 10017 Phone: (954) 341-5561 memert@ssbny.com
Cohen v. Wawa, Inc.	2:19-cv-06064	Richard M. Golomb, Esquire Kenneth J. Grunfeld, Esquire **GOLOMB & HONIK, P.C.** 1835 Market Street, Suite 2900 Philadelphia, PA 19103 Phone: (215) 985-9177	
Mullen et al. v. Wawa, Inc.	2:19-cv-06076	Linda P. Nussbaum Bart D. Cohen (PA 57606) James Perelman (P A 318456) **NUSSBAUM LAW GROUP P.C.** 1211 Avenue of the Americas 40th Floor	Michael E. Criden Lindsey C. Grossman **CRIDEN & LOVE, P.A.** 7301 SW 57th Court, Ste. 515 South Miami, FL 33143 (305) 357-9000

		New York, NY 10036-8718 (917) 438-9102 lnussbaum@nussbaumpc.com bcohen@nussbaumpc.com jperelman@nussbaumpc.com	mcriden@cridenlove.com lgrossman@cridenlove.com
Emery v. Wawa, Inc. et al.	2:19-cv-06077	Gary F. Lynch (PA ID 56887) Jamisen A. Etzel (PA ID 311554) Kevin W. Tucker (PA ID 312144) **CARLSON LYNCH, LLP** 1133 Penn Avenue, 5th Floor Pittsburgh, PA 15222 Tel. (412) 322-9243 glynch@carlsonlynch.com jetzel@carlsonlynch.com ktucker@carlsonlynch.com	
Hans-Arroyo v. Wawa, Inc.	19-cv-06127	Benjamin F. Johns Samantha E. Holbrook Mark B. DeSanto Andrew W. Ferich **CHIMICLES SCHWARTZ KRINER & DONALDSON SMITH LLP** One Haverford Centre 361 Lancaster Avenue Haverford, PA 19041 Tel: (610) 642-8500 bfj@chimicles.com seh@chimicles.com mbd@chimicles.com awf@chimicles.com	Tina Wolfson Bradley King Henry Kelston **AHDOOT & WOLFSON, PC** 10728 Lindbrook Drive Los Angeles, California 90024 Tel: (310) 474-9111 Fax: (310) 474-8585 twolfson@ahdootwolfson.com bking@ahdootwolfson.com hkelston@ahdootwolfson.com
Muller v. Wawa, Inc.	2:19-cv-06142	Sherrie R. Savett (PA Bar No. 17646) Shanon J. Carson (PA Bar No 85957) Jon J. Lambiras (PA Bar No 92384) **BERGER MONTAGUE, PC** 1818 Market Street, Suite 3600 Philadelphia, PA 19103 Tel: (215) 875-3000 Fax: (215) 875-4604 ssavett@bm.net scarson@bm.net jlambiras@bm.net	

		E. Michelle Drake **BERGER MONTAGUE, PC** 43 SE Main Street, Suite 505 Minneapolis, MN 55414 Tel: (612) 594-5933 Fax: (612) 584-4470 emdrake@bm.net	
Newton v. Wawa, Inc.	19-cv-06147	William B. Federman, *Pro Hac Vice Application to be Filed* **FEDERMAN & SHERWOOD** 10205 N. Pennsylvania Ave Oklahoma City, Oklahoma 73120 (405) 235-1560 (405) 239-2112 (facsimile) wbf@federmanlaw.com	
Roessle v. Wawa, Inc.	19-cv-06161	Sherrie R. Savett Shanon J. Carson Jon J. Lambiras **BERGER MONTAGUE, PC** 1818 Market Street, Suite 3600 Philadelphia, PA 19103 Telephone: (215) 875-3000 Facsimile: (215) 875-4604 ssavett@bm.net scarson@bm.net jlambiras@bm.net	Michael J. Gallagher, Jr Andrei V. Rado (*pro hac vice forthcoming*) **MILBERG PHILLIPS GROSSMAN, LLP** One Pennsylvania Plaza, Suite 1920 New York, NY 10119-0165 Telephone: (212) 594-5300 Facsimile: (212) 868-1229 mgallagher@milberg.com arado@milberg.com
Fisher v. Wawa, Inc.	19-cv-06179	**BARRACK, RODOS & BACINE** Julie B. Palley Chad A. Carder Jeffrey B. Gittleman Jeffrey W. Golan (PA #33729) 3300 Two Commerce Square 2001 Market Street Philadelphia, PA 19103	**BARRACK, RODOS & BACINE** Stephen R. Basser One America Plaza 600 W. Broadway, Suite 900 San Diego, CA 92101
Schultz v. Wawa, Inc.	19-06190	Natalie Finkelman Bennett (PA ID 57197) James C. Shah (PA ID 80337) Alec Berin (PA ID 328071) **SHEPHERD, FINKELMAN**	Mitchell A. Toups **MITCHELL A. TOUPS LTD** 2615 Calder Ave., Suite 400 Beaumont, TX 77702

		MILLER & SHAH, LLP 1845 Walnut Street, Suite 806 Philadelphia, PA 19103 Telephone: (610) 891-9880 Facsimile: (866) 300-7367 nfinkelman@sfmslaw.com jshah@sfmslaw.com Richard L. Coffman **THE COFFMAN LAW FIRM** Edison Plaza 350 Pine Street, Suite 700 Beaumont, TX 77701 Telephone: (409) 833-7700 Facsimile: (866) 835-8250 rcoffman@coffmanlawfirm.com	Telephone: (409) 838-0101 Facsimile: (409) 838-6780 matoups@wgttlaw.com Michael D. Shaffer (PA ID 60191) Michael H. Gaier (PA ID 50210) **SHAFFER & GAIER, LLC** 1628 JFK Boulevard, Suite 400 Philadelphia PA 19103 Telephone: (215) 751 0100 Facsimile: (215)751 0723 mshaffer@shaffergaier.com mgaier@shaffergaier.com

Dated: January 6, 2020

By: */s/ Eugene Spector*
Eugene Spector

JS 44 (Rev. 02/19) GEKP

CIVIL COVER SHEET

20-CV-100

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

20 100

I. (a) PLAINTIFFS

Demetrius Williams, individually & on behalf of all other similarly situated

(b) County of Residence of First Listed Plaintiff Camden, New Jersey
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Eugene A. Spector, Spector Roseman & Kodroff, 2001 Market St., Ste. 3420, Phila., PA 19103, 215-496-0300, espector@srkattorneys.com

DEFENDANTS

Wawa, Inc.

County of Residence of First Listed Defendant Delaware County, PA
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☒ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
28 U.S.C. §1332(d) - diversity of citizenship under Class Action Fairness Act

Brief description of cause:
Data breach - Negligence, Breach of Implied Contract, PA and NJ Unfair Trade Practices

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,000.00

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY *(See instructions)*:

JUDGE See attached list of related cases DOCKET NUMBER See attached list

DATE 01/06/2020

SIGNATURE OF ATTORNEY OF RECORD /s/ Eugene Spector

JAN - 6 2020

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

GEKP

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

20 100

DESIGNATION FORM

(to be used by counsel or pro se plaintiff to indicate the category of the case for the purpose of assignment to the appropriate calendar)

Address of Plaintiff: Camden, New Jersey

Address of Defendant: Wawa, Inc. 260 W. Baltimore Pike, Wawa, PA

Place of Accident, Incident or Transaction: Data breach took place at corporate headquarters in Wawa, PA

RELATED CASE, IF ANY:

Case Number: See attached list of cases Judge: See attached list Date Terminated: _____

Civil cases are deemed related when *Yes* is answered to any of the following questions:

1. Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court? Yes ☐ No ☐
2. Does this case involve the same issue of fact or grow out of the same transaction as a prior suit pending or within one year previously terminated action in this court? Yes ☑ No ☐
3. Does this case involve the validity or infringement of a patent already in suit or any earlier numbered case pending or within one year previously terminated action of this court? Yes ☐ No ☐
4. Is this case a second or successive habeas corpus, social security appeal, or pro se civil rights case filed by the same individual? Yes ☐ No ☐

I certify that, to my knowledge, the within case ☐ **is** / ☑ **is not** related to any case now pending or within one year previously terminated action in this court except as noted above.

DATE: 01/06/2020 (Must sign here) *Attorney-at-Law / Pro Se Plaintiff* PA Bar No. 13616 *Attorney I.D. # (if applicable)*

CIVIL: (Place a √ in one category only)

A. Federal Question Cases:

- ☐ 1. Indemnity Contract, Marine Contract, and All Other Contracts
- ☐ 2. FELA
- ☐ 3. Jones Act-Personal Injury
- ☐ 4. Antitrust
- ☐ 5. Patent
- ☐ 6. Labor-Management Relations
- ☐ 7. Civil Rights
- ☐ 8. Habeas Corpus
- ☐ 9. Securities Act(s) Cases
- ☐ 10. Social Security Review Cases
- ☐ 11. All other Federal Question Cases
  (Please specify): _____

B. Diversity Jurisdiction Cases:

- ☐ 1. Insurance Contract and Other Contracts
- ☐ 2. Airplane Personal Injury
- ☐ 3. Assault, Defamation
- ☐ 4. Marine Personal Injury
- ☐ 5. Motor Vehicle Personal Injury
- ☐ 6. Other Personal Injury *(Please specify):* _____
- ☐ 7. Products Liability
- ☐ 8. Products Liability – Asbestos
- ☑ 9. All other Diversity Cases
  (Please specify): Negligence - data breach

ARBITRATION CERTIFICATION

(The effect of this certification is to remove the case from eligibility for arbitration.)

I, Eugene A. Spector, counsel of record *or* pro se plaintiff, do hereby certify:

☑ Pursuant to Local Civil Rule 53.2, § 3(c) (2), that to the best of my knowledge and belief, the damages recoverable in this civil action case exceed the sum of $150,000.00 exclusive of interest and costs:

☐ Relief other than monetary damages is sought.

DATE: 01/06/2020 (Sign Here If Applicable) *Attorney-at-Law / Pro Se Plaintiff* PA Bar No. 13616 *Attorney I.D. # (if applicable)*

NOTE: A trial de novo will be a trial by jury only if there has been compliance with F.R.C.P. 38.

Civ. 609 (5/2018)

JAN - 6 2020

GEKP

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

CASE MANAGEMENT TRACK DESIGNATION FORM

Demetrius Williams	:	CIVIL ACTION
	:	20 100
v.	:	
	:	
Wawa, Inc.	:	NO.

In accordance with the Civil Justice Expense and Delay Reduction Plan of this court, counsel for plaintiff shall complete a Case Management Track Designation Form in all civil cases at the time of filing the complaint and serve a copy on all defendants. (See § 1:03 of the plan set forth on the reverse side of this form.) In the event that a defendant does not agree with the plaintiff regarding said designation, that defendant shall, with its first appearance, submit to the clerk of court and serve on the plaintiff and all other parties, a Case Management Track Designation Form specifying the track to which that defendant believes the case should be assigned.

SELECT ONE OF THE FOLLOWING CASE MANAGEMENT TRACKS:

(a) Habeas Corpus – Cases brought under 28 U.S.C. § 2241 through § 2255. ( )

(b) Social Security – Cases requesting review of a decision of the Secretary of Health and Human Services denying plaintiff Social Security Benefits. ( )

(c) Arbitration – Cases required to be designated for arbitration under Local Civil Rule 53.2. ( )

(d) Asbestos – Cases involving claims for personal injury or property damage from exposure to asbestos. ( )

(e) Special Management – Cases that do not fall into tracks (a) through (d) that are commonly referred to as complex and that need special or intense management by the court. (See reverse side of this form for a detailed explanation of special management cases.) (x)

(f) Standard Management – Cases that do not fall into any one of the other tracks. ( )

1/6/20	Eugene A. Spector	Pltf. Demetrius Williams
Date	**Attorney-at-law**	**Attorney for**
215-496-0300	215-496-6611	espector@srkattorneys.com
Telephone	**FAX Number**	**E-Mail Address**

(Civ. 660) 10/02

JAN - 6 2020

Related Cases

Case No.	Judge	Caption
2:19-cv-~~06109~~ 6019	Hon. Gene Pratter	Rapak v. Wawa, Inc.
2:19-cv-06032	Hon. Joel Slomsky	Kaufman v. Wawa, Inc.
2:19-cv-06064	Hon. Nitza Quinones Alejandro	Cohen v. Wawa, Inc.
2:19-cv-06076	Hon. Joel Slomsky	Mullen, Angelo & Bauman v. Wawa, Inc.
2:19-cv-06077	Hon. Darnell Jones	Emery v. Wawa, Inc. & Wild Goose Holdings, co.
2:19-cv-06127	Hon. Gene Pratter	Hans-Arroyo v. Wawa, Inc.
2:19-cv-06142	Hon. Wendy Beetlestone	Muller v. Wawa, Inc.
5:19-cv-06147	Hon. Gene Pratter	Newton v. Wawa, Inc.
19-cv-06161	Hon. Gene Pratter	Roessle v. Wawa, Inc.
19-cv-06179	Hon. Gene Pratter	Fisher v. Wawa, Inc.
19-cv-06190	Hon. Gene Pratter	Schultz v. Wawa, Inc.