UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

FIRST CHOICE FEDERAL CREDIT UNION, on Behalf of Itself and All Others Similarly Situated, **Plaintiff,** **v.** **WAWA, INC. and WILD GOOSE HOLDING CO., INC.,** **Defendants.**	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff First Choice Federal Credit Union ("Plaintiff"), on behalf of itself and all others similarly situated, asserts the following against Defendant WaWa, Inc. and Wild Goose Holding Co., Inc. (collectively, "WaWa" or "Defendants"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

I. INTRODUCTION

1. Plaintiff brings this class action on behalf of financial institutions that suffered, and continue to suffer, financial losses as a direct result of WaWa's conscious failure to take adequate and reasonable measures to protect its point-of-sale payment terminals, fuel dispensers, and payment processing servers. WaWa's actions left highly sensitive Payment Card Data, including, but not limited to, the cardholder name, credit or debit card number, and expiration date ("Payment Card Data") of Plaintiff's members exposed and accessible for use by hackers from at least March 4, 2019 through December 12, 2019, at which time WaWa claims the breach was contained. As a result, Plaintiff has and will incur significant damages in replacing members' payment cards and covering fraudulent purchases, among other things.

2. In or about March 2019, computer hackers accessed WaWa's inadequately protected point-of-sale systems and installed malicious software (often referred to as "malware") that infected potentially every WaWa in-store payment terminal and fuel dispenser in the United States.[1] Through this malware, hackers stole the Payment Card Data of an untold number of customers.[2]

3. The Data Breach was the inevitable result of WaWa's inadequate data security measures and lackadaisical approach to the security of its customers' Payment Card Data. Despite the well-publicized and ever-growing threat of cyber-attacks targeting Payment Card Data through vulnerable point-of-sale systems and inadequately protected computer networks, WaWa refused to implement certain best practices, failed to upgrade critical security systems, used outdated point-of-sale systems, ignored warnings about the vulnerability of its computer network, and disregarded and/or violated applicable industry standards.

4. WaWa's data security deficiencies were further buttressed by its failure to timely identify the Data Breach and subsequently contain it. By December 19, 2019, when WaWa first publicly acknowledged that a data breach compromising customer Payment Card Data had occurred, the Data Breach already had been ongoing for several months. The malware had remained undetected within WaWa's point-of-sale and computer systems from at least March 2019 until December 10, 2019, when WaWa first learned of the malware on its payment processing servers.

---

[1] WaWa, WaWa Notifies Customers of Data Security Incident, https://s3.amazonaws.com/wawa-kentico-prod/wawa/media/misc/wawa-data-security-incident-wire-release-12_19_2019.pdf (Dec. 19, 2019) (last accessed Dec. 23, 2019).

[2] Hereinafter, these events are referred to as the "WaWa Data Breach" or "Data Breach."

5. In its December 19, 2019 press release, WaWa disclosed the Data Breach "affected customer payment card information used at potentially all WaWa locations[.]"[3]

6. The financial costs caused by WaWa's deficient data security approach have been and will be borne primarily by financial institutions, like Plaintiff, that issued the payment cards compromised in the Data Breach. These costs include, but are not limited to, canceling and reissuing compromised cards and reimbursing their members/customers for fraudulent charges. Moreover, the duration of the Data Breach has and will cause Plaintiff and other members of the Class to suffer many millions of dollars more in damages than they would have suffered had WaWa had an adequate process in place to detect and contain the data breach.

7. This class action is brought on behalf of financial institutions throughout the U.S. to recover the damages that they and others similarly situated have suffered, and continue to suffer, as a direct result of the WaWa Data Breach. Plaintiff asserts claims for negligence, negligence *per se*, and declaratory and injunctive relief.

II. PARTIES

A. Plaintiff

8. Plaintiff First Choice Federal Credit Union is a citizen of the Commonwealth of Pennsylvania. Plaintiff is a federally chartered credit union with its principal place of business located in New Castle, Pennsylvania. As a result of the WaWa Data Breach, Plaintiff First Choice Federal Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the Data Breach, costs to refund fraudulent charges, costs

[3] WaWa, An Open Letter from WaWa CEO Chris Gheysens to Our Customers, https://www.wawa.com/alerts/data-security (Dec. 19, 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.") (last accessed Dec. 23, 2019).

to investigate fraudulent charges, and costs due to lost interest and transaction fees due to reduced card usage.

9. Plaintiff is at risk of imminent and certain impending injury as a result of recurrent fraudulent transactions on payment cards linked to the WaWa Data Breach. Furthermore, time will tell whether Plaintiff is subject to an imminent threat of future harm because WaWa's response to the Data Breach is so inadequate that it is doubtful that it has cured the deficiencies in its data security measures sufficiently to prevent a subsequent data breach.

B. Defendants

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

11. Defendant Wild Goose Holding Co., Inc. is a Delaware corporation. Its principal place of business is also in WaWa, Pennsylvania and it too is a Pennsylvania citizen. Defendant Wild Goose Holding Co., Inc. is WaWa, Inc.'s parent company.

12. WaWa is engaged in the business of developing and operating a system of convenience stores. WaWa currently operates more than 850 retail stores throughout Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida, and Washington, D.C. WaWa offers gasoline at over 600 of these locations.[4] According to Forbes magazine, WaWa ranked 25th on the list of largest private companies in 2019, with a total revenue of $12.1 billion.[5]

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

---

[4] WaWa, About WaWa, https://www.wawa.com/about (last accessed Dec. 20, 2019).

[5] Forbes, #25 WaWa, https://www.forbes.com/companies/wawa/#35178b652644 (last accessed Dec, 20, 2019).

III. JURISDICTION AND VENUE

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

15. This Court has personal jurisdiction over Defendants named in this action because Defendants are headquartered within, and conduct substantial business in, Pennsylvania and this District through its convenience stores and commercial website.

16. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendants are headquartered in this District and a substantial part of the events, errors, omissions, and decisions leading to the Data Breach occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Payment Card Processing Background

17. It is well known that customer Payment Card Data is valuable and often targeted by hackers. Over the last several years, numerous data breaches have occurred at large retailers and restaurants nationwide, including Wendy's, The Home Depot, Target, Kmart, P.F. Chang's, and many others. Despite widespread publicity and industry alerts regarding these other notable data breaches, WaWa failed to take reasonable steps to adequately protect its computer systems from being breached.

18. A large portion of WaWa's sales are made to customers who use credit or debit cards. When a customer uses a credit or debit card, the transaction involves four primary parties: (1) the "merchant" (*e.g.*, WaWa) where the purchase is made; (2) an "acquiring bank" (which typically is a financial institution that contracts with the merchant to process its payment card

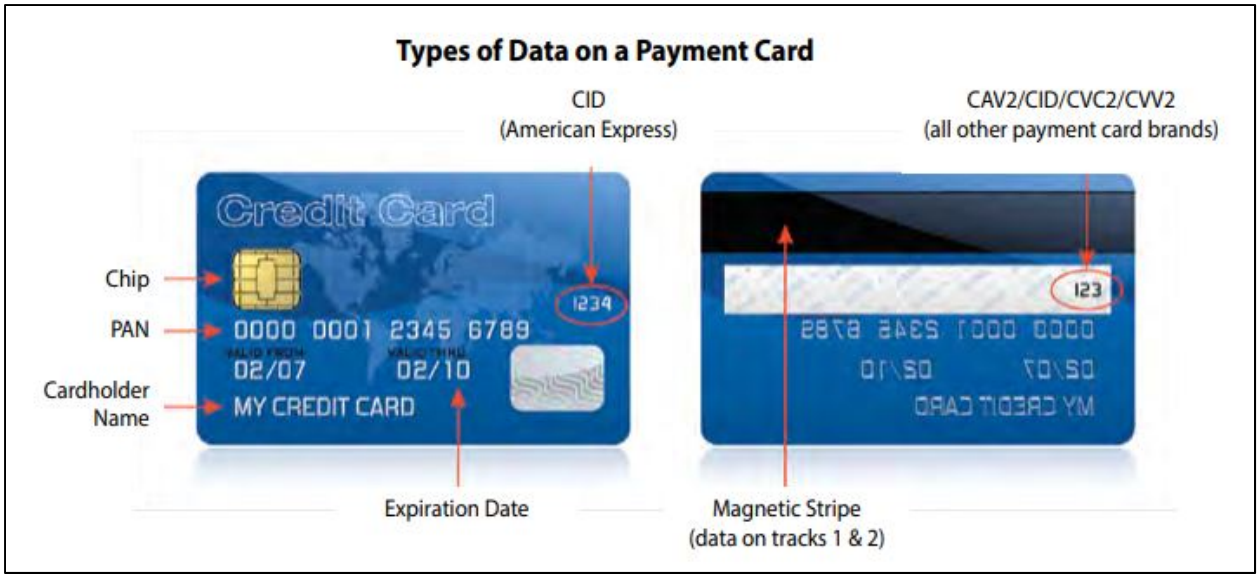
transactions); (3) a "card network" or "payment processor" (such as Visa and MasterCard); and (4) the "issuer" (which is a financial institution – such as Plaintiff – that issues credit and debit cards to its members/customers).

19. Processing a payment card transaction involves four major steps:

- *Authorization* – when a customer presents a card to make a purchase, WaWa requests authorization of the transaction from the card's issuer;
- *Clearance* – if the issuer authorizes the transaction, WaWa completes the sale to the customer and forwards a purchase receipt to the acquiring bank with which it has contracted;
- *Settlement* – the acquiring bank pays WaWa for the purchase and forwards the receipt to the issuer, which then reimburses the acquiring bank; and
- *Post-Settlement* – the issuer posts the charge to the customer's credit or debit account.

20. In processing payment card transactions, merchants acquire a substantial amount of information about each customer, including his or her full name; credit or debit card account number; card security code (the value printed on the card or contained in the microprocessor chip or magnetic strip of a card and used to validate card information during the authorization process); the card's expiration date and verification value; and the PIN number for debit cards.[6]

[6] *See* PCI Security Standards Council, *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1*, 11, July 2018, https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf (last accessed Dec. 22, 2019).



21. Merchants typically store this information on their computer systems and transmit it to third parties to complete the transaction. At other times, and for other reasons, merchants may also collect other personally identifiable information about their customers, including, but not limited to, financial data, mailing addresses, phone numbers, driver's license numbers, and email addresses.

22. For years, WaWa has obtained massive amounts of customer Payment Card Data. WaWa uses this information to process payment card transactions in connection with sales to its customers. Customer Payment Card Data is an asset of considerable value to both the WaWa and to hackers, who can easily sell this data, as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[7]

23. WaWa is—and at all relevant times has been—aware that the Payment Card Data it obtains and processes is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases. To this end, WaWa

[7] *The Value of a Hacked Company*, KREBS ON SECURITY (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last accessed Dec. 20, 2019).

posted a job opening on or about December 4, 2019—just days before allegedly discovering the WaWa Data Breach—seeking an Information Security Incident Response Junior Analyst to "follow the processes and procedures necessary for the detection, response and remediation of cyber related attacks on the Wawa enterprise."[8]

24. WaWa also is—and at all relevant times has been—aware of the importance of safeguarding its customers' Payment Card Data and of the foreseeable consequences that would occur if its data security systems were breached, specifically including the fraud losses and theft that would be imposed on consumers, such as Plaintiff. Indeed, WaWa's December 4, 2019 job posting also requires the successful applicant have a "[v]ery basic understanding of relevant legal and regulatory requirements, such as: Payment Card Industry Data Security Standard." *Id*.

25. In addition to its general duty to act reasonably in handling and safeguarding customers' Payment Card Data to prevent the risk of foreseeable harm to others, WaWa is—and at all relevant times has been—obligated to safeguard such information by, among other things, industry standards, federal law, and its own commitments, internal policies, and procedures.

B. The WaWa Data Breach: March 2019 to Present

26. Beginning as early as March 2019, computer hackers took advantage of vulnerabilities in WaWa's computer and point-of-sale systems to install malware that ultimately infected potentially every WaWa location in the United States. Through this malware, the hackers were able to steal WaWa's customers' Payment Card Data that WaWa had collected in conjunction with its customers' purchases.

[8] Indeed, WaWa Information Security Incident Response Junior Analyst, https://www.indeed.com/viewjob?jk=7a1f2ac3eeb48eea&tk=1dsibai40p2p0800&from=serp&vjs=3 (posted Dec. 3, 2019) (last accessed Dec. 20, 2019) (copy saved by Plaintiff's counsel).

27. On December 19, 2019 (approximately ten months after hackers first installed malware on its computer processors), WaWa announced that it was investigating a theft its customers' Payment Card Data. WaWa explained, "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."[9]

28. Taking advantage of WaWa's lax data security and delay in discovering the malware on its servers, hackers were able to gather large amounts of Payment Card Data. With that Payment Card Data, unknown perpetrators are now capable of making undetected fraudulent purchases on credit and debit cards belonging to Plaintiff and members of the Class. Unknown perpetrators are also capable of specifically targeting and draining debit accounts with large amounts of money in them belonging to Plaintiff and members of the Class. By failing to timely identify that its systems had been subjected to a data breach, WaWa allowed hackers to have unfettered access to WaWa's computer and point-of-sale systems to obtain customers' Payment Card Data for at least ten months, thereby exponentially increasing the harm suffered by Plaintiff and members of the Class.

29. Up to, and including, the period during which the WaWa Data Breach occurred, WaWa's data security systems suffered from many deficiencies that made them susceptible to hackers, including, without limitation, the following:

[9] WaWa, WaWa Data Security – Updates & Customer Resources, https://www.wawa.com/alerts/data-security (Dec. 19, 2019) (last accessed Dec. 20, 2019).

a. WaWa's IT management were unqualified and failed to maintain a system of accountability over data security, thereby knowingly allowing data security deficiencies to persist;

b. WaWa ignored well-known warnings that its point-of-sale system was susceptible to data breach;

c. WaWa failed to implement certain protocols that would have prevented unauthorized programs, such as malware, from being installed on its point-of-sale and other systems that accessed Payment Card Data and otherwise would have protected Payment Card Data; and

d. WaWa failed to install software to adequately track access to its network, monitor the network for unusual activity, and prevent exfiltration of data, which would have detected the presence of hackers and prevented Payment Card Data from being stolen.

30. Attempting to downplay the seriousness of the Data Breach, WaWa assured its customers that "anyone impacted [ ] will not be responsible for fraudulent charges related to this incident." [10] In a separate letter to customers, WaWa's CEO, Chris Gheysens wrote, "I want to reassure you that you will not be responsible for any fraudulent charges on your payment cards related to this incident[.]"[11] WaWa has not provided any assurances to Plaintiff and similarly situated payment card issuers who will lose millions of dollars as a result of having to cancel and reissue cards compromised in the WaWa Data Breach, refund fraudulent charges incurred by their

[10] Wawa, WaWa Notifies Customers of Data Security Incident, https://s3.amazonaws.com/wawa-kentico-prod/wawa/media/misc/wawa-data-security-incident-wire-release-12_19_2019.pdf (Dec. 19, 2019) (last accessed Dec. 20, 2019).

[11] Wawa, An Open Letter from WaWa CEO Chris Gheysens to Our Customers, https://www.wawa.com/alerts/data-security (Dec. 19, 2019) (last accessed Dec. 20, 2019).

members/customers, investigate fraudulent charges, and the lost interest and transaction fees due to reduced card usage.

31. Beginning on Friday, December 27, 2019, Visa issued a series of Compromised Account Management System ("CAMS") alerts to Plaintiff, indicating that the estimated fraud "exposure window" for the WaWa Data Breach ran from April 22, 2019 through December 13, 2019. The CAMS alert further indicated that both Track 1 and Track 2 data, which generally includes credit and debit card information, such as cardholder name, primary account number, and expiration date may have been compromised in the Data Breach. According to the CAMS alerts received by Plaintiff, at least 65 payment cards issued by Plaintiff to its members were compromised as a result of the WaWa Data Breach.

C. WaWa Failed to Comply with Its Duties

1. WaWa Failed to Comply with Industry Standards for Data Security

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

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

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

[12] PCI Security Standards Council, *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1*, 9, July 2018,

The PCI Data Security Standard

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data and/or sensitive authentication data. It consists of steps that mirror security best practices.

Goals	PCI DSS Requirements
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

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

36. Among other things, PCI DSS 3.2.1 requires WaWa to properly secure Payment Card Data; not store cardholder data beyond the time necessary to authorize a transaction; to timely upgrade its point-of-sale software; implement proper network segmentation; encrypt Payment Card Data at the point-of-sale; restrict access to Payment Card Data to those with a need to know;

https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf (last accessed Dec. 22, 2019).

and establish a process to identify; and timely fix security vulnerabilities. Upon information and belief, WaWa failed to comply with each of these requirements.

2. WaWa Failed to Comply with Federal Trade Commission Requirements

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

38. 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.

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

40. 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 in regard to their data security obligations.

41. In the years leading up to the WaWa Data Breach, and during the course of the breach itself, WaWa failed to follow the guidelines set forth by the FTC and actively mishandled the management of its IT security. Furthermore, by failing to have reasonable data security measures in place, WaWa engaged in an unfair act or practice within the meaning of §5 of the FTC Act.

3. The Data Breach Damaged Financial Institutions

42. WaWa failed to protect its customers' Payment Card Data and as a result, Plaintiff and Class members have and will suffer millions of dollars in damages

43. WaWa failed to follow industry standards and failed to effectively monitor its point-of-sale and security systems to ensure the safety of customer information. WaWa's substandard security protocols, improper retention of cardholder data, and failure to regularly monitor for unauthorized access caused customers' Payment Card Data to be compromised for months without detection by WaWa.

44. The Data Breach caused or will cause substantial damage to Plaintiff and Class members, who are acting immediately to mitigate the risk of a massive number of fraudulent transactions being made on payment cards that they issued while simultaneously taking steps to prevent future fraud. Consumers are ultimately protected from most fraud loss, but Plaintiff and Class members are not. Financial institutions, like Plaintiff and other Class members, bear primary responsibility for reimbursing members/customers for fraudulent charges and covering the cost of issuing new cards for members/customers to use.

45. As a result of the WaWa Data Breach, Plaintiff and Class members are required, and will continue to be required, to cancel and reissue payment cards, change or close accounts, notify members/customers that their cards were compromised, investigate claims of fraudulent

activity, refund fraudulent charges, increase fraud monitoring on potentially impacted accounts, and take other steps to protect themselves and their members/customers. Plaintiff and members of the Class also lost or will lose interest and transaction fees due to reduced card usage. Furthermore, debit and credit cards belonging to Plaintiff and Class members—as well as the account numbers on the face of the cards—were devalued.

46. The financial damages suffered by Plaintiff and members of the Class are significant and ongoing.

V. CLASS ACTION ALLEGATIONS

47. Plaintiff brings this action on behalf of itself and as a class action, pursuant to the provisions of Rules 23(a), 23(b)(2), and 23(b)(3) of the Federal Rules of Civil Procedure, on behalf of the following class (the "Class"):

> All banks, credit unions, financial institutions, and other entities in the United States (including its Territories and the District of Columbia) that issued payment cards (including debit or credit cards) used by consumers to make purchases from WaWa from March 4, 2019 to December 13, 2019.[13]

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

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

[13] As evidence is developed, Plaintiff may amend the class definition or class period if necessary to accurately correspond to the relevant details of the Data Breach.

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

50. **Numerosity:** All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiff is informed and believes that there are hundreds of members of the Class, the precise number of Class members is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

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

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

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

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

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

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

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

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

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

52. **Typicality:** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiff is a member of the Class, having issued payment cards that were compromised in the WaWa Data Breach. Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through Defendants' conduct.

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

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

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

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

VI. CHOICE OF LAW

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

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

58. Upon information and belief, control over WaWa's point-of-sale systems and IT personnel is exercised at WaWa's headquarters in Pennsylvania. To this end, WaWa currently is hiring an Information Security Incident Response Junior Analyst based in WaWa, Pennsylvania,

to "follow the processes and procedures necessary for the detection, response and remediation of cyber related attacks on the Wawa enterprise."[14]

59. Pennsylvania, which seeks to protect the rights and interests of Pennsylvania and other U.S. businesses against a company doing business in Pennsylvania, has a greater interest in the claims of Plaintiff and the Class members than any other state and is most intimately concerned with the outcome of this litigation.

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

VII. CAUSES OF ACTION

COUNT I
Negligence
On behalf of the Plaintiff and the Class

61. Plaintiff incorporates by reference all preceding allegations, as though fully set forth herein.

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

---

[14] Indeed, WaWa Information Security Incident Response Junior Analyst, https://www.indeed.com/viewjob?jk=7a1f2ac3eeb48eea&tk=1dsibai40p2p0800&from=serp&vjs=3 (posted Dec. 3, 2019) (last accessed Dec. 20, 2019) (copy saved by Plaintiff's counsel).

63. WaWa has a common law duty to prevent the foreseeable risk of harm to others, including Plaintiff and the Class. It was certainly foreseeable to WaWa that injury would result from a failure to use reasonable measures to protect Payment Card Data and to provide timely notice that a breach was detected. It was also foreseeable that, if reasonable security measures were not taken, hackers would steal Payment Card Data belonging to millions of WaWa's customers; thieves would use Payment Card Data to make large numbers of fraudulent transactions; financial institutions would be required to mitigate the fraud by cancelling and reissuing the compromised cards and reimbursing their members/customers for fraud losses; and that the resulting financial losses would be immense.

64. WaWa assumed the duty to use reasonable security measures as a result of its conduct.

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

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

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

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

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

b. failure to employ systems to protect against malware;

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

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

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

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

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

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

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

70. As a direct and proximate result of WaWa's negligence, Plaintiff and members of the Class have or will suffer injury, including, but not limited to, cancelling and reissuing payment cards, changing or closing accounts, notifying members/customers that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their members/customers. Plaintiff and the Class also lost or will lose interest and transaction fees, due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

COUNT II
Negligence *Per Se*
On behalf the Plaintiff and the Class

71. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

72. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as WaWa, of failing to use reasonable measures to protect Payment Card Data. The FTC publications and orders described above also form part of the basis of WaWa's duty.

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

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

75. Plaintiff and members of the Class are within the class of persons that §5 of the FTC Act (and similar state statutes) was intended to protect, as they are engaged in trade and commerce and bear primary responsibility for directly reimbursing consumers for fraud losses. Moreover, many of the Class members are credit unions, which are organized as cooperatives whose members are consumers.

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

77. As a direct and proximate result of WaWa's negligence *per se*, Plaintiff and the Class have or will suffer injury, including, but not limited to, cancelling and reissuing payment cards, changing or closing accounts, notifying members/customers that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their members/customers. They also lost or will lose interest and transaction fees, due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

COUNT III
Declaratory and Injunctive Relief
On behalf of Plaintiff and the Class

200. Plaintiff incorporates by reference all preceding allegations, as though fully set forth herein.

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

202. An actual controversy has arisen in the wake of WaWa's Data Breach regarding its common law and other duties to reasonably safeguard Payment Card Data. Plaintiff alleges that WaWa's data security measures were inadequate and remain inadequate. Furthermore, Plaintiff continues to suffer injury as additional fraudulent charges may be made on payment cards it issued to WaWa's customers.

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

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

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

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

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

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

b. implement encryption keys in accordance with industry standards;

c. implement EMV technology;

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

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

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

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

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

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

206. The hardship to Plaintiff and the Class, if an injunction is not issued, exceeds the hardship to WaWa, if an injunction is issued. Among other things, if another massive data breach occurs at WaWa, Plaintiff and members of the Class will likely incur hundreds of millions of dollars in damage. On the other hand, the cost to WaWa of complying with an injunction by employing reasonable data security measures is relatively minimal and WaWa has a pre-existing legal obligation to employ such measures.

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

PRAYER FOR RELIEF

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

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

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

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

D. Grant Plaintiff the injunctive relief requested;

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

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

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of any and all issues in this action so triable.

Dated: January 3, 2020

Respectfully submitted,

CARLSON LYNCH, LLP

/s/ Gary F. Lynch

Gary F. Lynch (PA ID 56887)
Jamisen A. Etzel (PA ID 311554)
Kevin W. Tucker (PA ID 312144)
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Tel. (412) 322-9243
glynch@carlsonlynch.com
jetzel@carlsonlynch.com
ktucker@carlsonlynch.com

LOWEY DANNENBERG, P.C.
Vincent Briganti (*pro hac vice* forthcoming)
Christian Levis (*pro hac vice* forthcoming)
Johnathan Seredynski (*pro hac vice* forthcoming)
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
vbriganti@lowey.com
clevis@lowey.com
jseredynski@lowey.com

LOWEY DANNENBERG, P.C
Anthony M. Christina (PA ID# 322528)
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Telephone: (215) 399-4770
achristina@lowey.com

LOCKRIDGE GRINDAL NAUEN P.L.L.P.
Karen H. Riebel
Kate M. Baxter-Kauf
100 Washington Avenue S, Suite 2200
Minneapolis, MN 55401
Tel. (612) 339-6900
Fax (612) 339-0981
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com

CHESTNUT CAMBRONNE PA
Bryan L. Bleichner
Jeffrey D. Bores
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
(612)339-7300
bbleichner@chestnutcambronne.com
jbores@chestnutcambronne.com

LEVIN SEDRAN & BERMAN, LLP
Charles E. Schaffer
Frederick S. Longer
510 Walnut Street – Suite 500
Philadelphia, PA 19106-3697
Phone: (215) 592-1500
Fax: (215) 592-4663
cschaffer@lfsblaw.com

Counsel for Plaintiff