UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

GREATER CHAUTAUQUA FEDERAL CREDIT UNION, individually and on behalf of a class of similarly situated financial institutions, Plaintiff, v. WAWA, INC. and WILD GOOSE HOLDING CO., INC., Defendants.	:	Case No: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Greater Chautauqua Federal Credit Union ("GCFCU" or "Plaintiff") by its undersigned counsel, individually and on behalf of a class of similarly situated financial institutions, upon personal knowledge as to itself and its own acts, and upon information and belief and investigation by Plaintiff's counsel (which included, among other things, a review of public documents as to all other matters), brings this action against Defendants Wawa Inc. ("Wawa") and Wild Goose Holding Co., Inc. ("Wild Goose") (collectively the "Defendants") and alleges the following:

NATURE OF THE ACTION

1. This is a class action on behalf of credit unions, banks, and other financial institutions that suffered injury as a result of a security breach at Wawa's post-of-sale payment terminals, fuel dispensers, and payment processing servers beginning on or around March 2019 and continuing through December 2019 (hereinafter the "Wawa Data Breach"). The Wawa Data Breach compromised the names, credit and debit card numbers, card expiration dates, and likely

card verification values ("CVVs"), and other credit and debit card information of millions Wawa customers.

2. Wawa is an American chain of convenience stores and gas stations located along the East Coast of the United States, operating in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Washington, D.C., and Florida. In December 2019, it announced one of the largest breaches of credit card data in history.

3. The Wawa Data Breach forced Plaintiff and other financial institutions to:

a. cancel or reissue any credit and debit cards affected by the Wawa Data Breach;

b. close any deposit, transaction, checking, or other accounts affected by the Wawa Data Breach, including but not limited to stopping payments or blocking transactions with respect to the accounts;

c. open or reopen any deposit, transaction, checking, or other accounts affected by the Wawa Data Breach;

d. refund or credit any cardholder to cover the cost of any unauthorized transaction relating to the Wawa Data Breach;

e. respond to a higher volume of cardholder complaints, confusion, and concern;

f. increase fraud monitoring efforts; and/or

g. lose revenue as a result of a decrease in card usage after the breach was disclosed to the public.

4. Defendants' failure to maintain adequate computer data security directly and proximately caused Plaintiff's injuries. Defendants failed to adequately protect customer

information including credit and debit card data and personal identifying information ("PII"). Defendants failed to employ adequate security measures despite the known threat of attacks by third parties using malware and other malicious software to gather sensitive information, as has been well-publicized after data breaches at large national retail and restaurant chains in recent years including, among others, Target, Home Depot, Sally Beauty, Harbor Freight Tools, P.F. Chang's, Kmart, Eddie Bauer, Noodles & Co., and Neiman Marcus.

5. Indeed, in November 2019, just weeks before Wawa announced the Breach, Visa (the nation's largest credit card network) warned that hackers were specifically targeting fuel dispensers (such as Wawa) to steal payment card information. Visa reported that gas stations emerged as attractive targets for cybercriminals because many have been slow to adopt more-secure payment-processing technology. Specifically, Visa said the attacks could continue as long as gas stations used magnetic-stripe readers to accept card payments (as Wawa did), instead of devices that take cards equipped with computer chips. Unfortunately, Visa's prediction became true.

6. Defendants' failure to adequately secure their data was inexcusable. The Wawa Data Breach involved most of the same techniques as those used in major data breaches in the preceding months and years. Nevertheless, despite having knowledge that such data breaches were occurring (and particularly targeted at gas stations), Defendants failed to adequately protect sensitive payment card information and caused damage to Plaintiff and other similarly situated financial institutions.

7. Not only did Defendants fail to prevent the intrusion, but they compounded the injury by failing to detect or notify customers and financial institutions of the infiltration for a period of at least nine months, allowing hackers unfettered access to Wawa's payment systems.

8. According to Defendants' security experts, the Wawa data systems were infected with a form of malware that its antivirus systems failed to detect. As such, the volume of data stolen was much greater than it would have been had Defendants maintained adequate antivirus software systems to identify and eliminate the breach at the time it occurred.

9. On December 19, 2019, Wawa first announced that its payment data systems had been breached. Wawa claims it first learned of the malware intrusion on December 10, 2019. Wawa explained on December 19, 2019, that "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." Defendants did not disclose the scale of the breach, the number of cards compromised, or the nature of the malware used.

10. On January 28, 2020, cyber-security expert Brian Krebs noted that fraud experts have begun to see the first batch of card data stolen from Wawa customers being sold on the dark web at one of the popular internet fraud bazaars known as "Joker's Stash."[1] At the commencement of the sale of this first batch of card data, Joker's Stash noted the cards were from "a huge nationwide breach" that includes more than 30 million cards issued by thousands of financial institutions across more than forty states.

11. According to Gemini Advisory, a fraud intelligence company, the biggest concentrations of stolen cards from the first batch of cards being sold map back to Wawa customer cards in Florida and Pennsylvania.[2] Gemini Advisory also noted that banks with nationwide presence and "financial institutions along the East Coast had significant exposure." Gemini

[1] https://krebsonsecurity.com/2020/01/wawa-breach-may-have-compromised-more-than-30-million-payment-cards/.
[2] *Id.*

Advisory wrote that since "the breach may have affected over 850 stores and potentially exposed 30 million sets of payment records, it ranks among the largest payment card breaches of 2019, and of all time."

12. As a direct and proximate result of Defendants' tortious conduct, vast amounts of financial and customer information were stolen from the Wawa payment processing network. The data stolen in the breach allows thieves to create counterfeit copies of the stolen cards. Though an investigation is still ongoing, it appears that credit and debit card data from tens of millions of accounts of Defendants' Wawa customers has been stolen. Plaintiff and members of the Class have incurred and will continue to incur significant damages associated with, among other things:

a. notifying their customers of issues related to the Wawa Data Breach;

b. costs for cancelling and reissuing thousands of credit and/or debit cards;

c. costs for reimbursing their customers for fraudulent charges, including, but not limited to issuing refunds or credits to affected customers;

d. voiding deposits and transactions and closing checking or other accounts affected by the breach, including, but not limited to stopping payments or blocking transactions with respect to affected accounts;

e. handling a higher-than-usual number of customer service inquiries; and

f. conducting investigations related to the breach.

13. Plaintiff and the members of the Class seek to recover damages caused by Defendants' negligence, negligence *per se*, and unfair competion.

JURISDICTION AND VENUE

14. This Court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d), in that: (a) the Class has more than 100 Class members; (b) the amount at issue exceeds

five million dollars ($5,000,000.00), exclusive of interest and costs; and (c) minimal diversity exists as Plaintiff and Defendants are citizens of different states. Plaintiff Greater Chautauqua Federal Credit Union is a citizen of New York. Defendant Wawa is a citizen of New Jersey, where it is incorporated, and Pennsylvania, where its principal place of business is located. Defendant Wild Goose is a citizen of Delaware, where it is incorporated and where its principal place of business is located.

15. Venue in the United States District Court for the Eastern District of Pennsylvania appropriate, pursuant to 28 U.S.C. §1391, in that Defendants maintain their principal places of business in this District, regularly transact business in this District, and a substantial part of the events giving rise to this claim arose in this District.

PARTIES

16. Plaintiff Greater Chautauqua Federal Credit Union is a chartered federal credit union whose main offices are located in Falconer, NY, just north of the Pennsylvania border.

17. Plaintiff provided its customers with credit and/or debit cards equipped with magnetic strips containing sensitive financial data. Plaintiff's customers used these cards to engage in financial transactions at Defendants' stores.

18. As a direct result of the Wawa Data Breach, Plaintiff incurred damages. These costs are ongoing, as Plaintiff continues to investigate the breach, replace impacted cards, and/or investigate and pay for fraudulent transactions caused by the data breach.

19. Defendant Wawa is a New Jersey corporation with its principal place of business located at 260 W. Baltimore Pike, Media, PA 19063. Wawa operates a chain of retail convenience stores and gas stations. Wawa has approximately 850 stores in Pennsylvania, New Jersey,

Delaware, Maryland, Virginia, Florida, and the District of Columbia, all of which were impacted by the breach.

20. Wawa serves 800 million customers annually and has annual revenues over $12 billion.

21. Defendant Wild Goose is a Delaware corporation with its principal place of business located at 1105 N Market Street, Suite 936, Wilmington, DE 19801. Wild Goose is the parent holding company of Defendant Wawa.

FACTUAL ALLEGATIONS

Background on Electronic Debit and Credit Card Transactions

22. Plaintiff and the members of the Class are financial institutions that issue payment cards (*e.g.*, debit or credit cards branded with the VISA or MasterCard logo) to their customers. Plaintiff's customers used these cards to make purchases at Wawa stores during the period of the Wawa Data Breach.

23. Wawa stores accept customer payment cards for the purchase of goods and services. At the point of sale ("POS"), these cards are swiped on a POS terminal, and either a personal identification number (or some other confirmation number) is entered or a receipt is signed to finish the transaction on behalf of the customer.

24. A typical credit or debit card transaction made on a credit card network is processed through a merchant (where the initial purchase is made), an acquiring bank (which is typically a financial institution that contracts with a merchant to process its credit card and debit card transactions and is a member of the credit card associations), a processor (a company that handles payment transactions between by relaying the credit card information from the customer to the merchant's bank account), and an issuer (which is a financial institution like Plaintiff and members

of the proposed Class that issues credit cards and debit cards to consumers and is a member of the credit card associations). When a purchase is made using a credit card or debit card on a credit card network, the merchant seeks authorization from the issuer for the transaction. In response, the issuer informs the merchant whether it will approve or decline the transaction. Assuming the transaction is approved, the merchant processes the transaction and electronically forwards the receipt directly to the acquiring bank. The acquiring bank then pays the merchant, forwards the final transaction data to the issuer, and the issuer reimburses the acquiring bank. The issuer then posts the charge to the consumer's credit card or debit card account.

25. Given the extensive network of financial institutions involved in these transactions and the sheer volume of daily transactions using credit and debit cards, financial institutions and credit card processing companies have issued rules and standards governing the basic measures and protections that merchants must take to ensure consumers' valuable data is protected.

26. First, the card processing networks issue regulations ("Card Operating Regulations") that are enforceable upon Defendants as a condition of Defendants' contract with the acquiring bank. The Card Operating Regulations generally prohibit Defendants (or any merchant) from disclosing any cardholder account numbers, personal information, magnetic stripe information, or transaction information to third parties other than the merchant's agent, the acquiring bank, or the acquiring bank's agents. Under the Card Operating Regulations, Defendants are ***required*** to maintain the security and confidentiality of debit and credit cardholder information and magnetic stripe information and protect it from unauthorized disclosure.

27. Similarly, the Payment Card Industry Data Security Standards ("PCI DSS") is a list of 12 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 Defendants 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.

28. The 12 requirements of the PCI DSS are:

Build and Maintain a Secure Network and Systems

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- Protect all systems against malware and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Restrict access to cardholder data by business need to know
- Identify and authenticate access to system components
- Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an Information Security Policy

- Maintain a policy that addresses information security for all personnel.[3]

29. Defendants were at all times fully aware of their data protection obligations, which emanated from their participation in the payment card processing networks and their daily collection and transmission of millions of sets of payment card data.

30. As a result of their participation in the payment card processing networks, Defendants knew that their customers and the financial institutions which issued the payment cards to the customers were trusting that Defendants would keep their customers' sensitive financial information secure from data thieves.

31. Furthermore, Defendants knew that if they failed to secure their customers' sensitive financial information, the financial institutions issuing the payment cards to their customers, *i.e.*, Plaintiff and other Class members, would suffer harm by having to notify customers, close out and open new customer accounts, reissue customers cards and/or refund customers' losses resulting from the unauthorized use of their accounts, and suffer lost revenues as a result of decreased usage of their customers' debit/credit cards.

32. Plaintiff believes that the deficiencies in Wawa's security system included a lack of basic security measures that IT professionals would identify as problematic.

33. Specifically, some of the security flaws identified in the Wawa Data Breach were explicitly highlighted by VISA as early as 2009, when it issued a Data Security Alert describing the threat of RAM scraper malware.[4] The report instructs companies to:

---

[3] The PCI DSS 12 core security standards can be found at: https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security (last accessed February 12, 2020).

[4] The report can be found at: https://www.firstdata.com/downloads/partners/fd_gpm_notice_visa_security_alert_28may09_partnersupport.doc (last visited February 12, 2020).

- Secure your remote access connectivity
- Implement a secure network configuration including egress and ingress filtering to only allow the ports/services necessary to conduct business. Organizations that use a MultiProtocol Lambda Switching (MPLS) topology for shared network and protocol switching should take steps to secure their MPLS environments. View the Complete Guide for Securing MPLS Networks on ZDNet.com
- Utilize host-based Intrusion Detection Systems (IDS)
- Monitor firewalls for suspicious traffic (particularly outbound traffic to unknown addresses)
- Implement file integrity monitoring
- Secure systems so that unauthorized software cannot be installed
- Ensure that all anti-virus and anti-spyware software programs are up-to-date
- Routinely examine systems and networks for newly-added hardware devices; unknown files and software
- Periodically reboot your POS systems to clear volatile memory
- If you detect a suspected or confirmed security breach, notify your acquiring bank immediately.

34. More recently, Visa warned Fuel Dispenser Merchants, such as Wawa, of the following:[5]

Recommendations for Fuel Dispenser Merchants

[5] The report can be found at: https://usa.visa.com/dam/VCOM/global/support-legal/documents/visa-security-alert-attacks-targeting-fuel-dispenser-merchant-pos.pdf (last visited February 12, 2020).

Fuel dispenser merchants should deploy terminals that support chip wherever possible to deter attacks targeting POS environments, as well as the fraud that occurs at non-chip POS terminals. As a reminder, after the Visa October 2020 chip liability shift date, the responsibility for counterfeit fraud will shift to the fuel dispenser merchants who have not enabled chip acceptance.

Visa recommends fuel dispenser merchants take the following actions to mitigate against these threats:

• **Deploy and enable chip acceptance** on all point-of-sale devices.

• **Deploy Point-to-Pont Encryption (P2PE).**

• **Employ the IOCs contained in this report** to detect, remediate, and prevent attacks using the POS malware variant.

• **Educate employees about cyber threats and phishing.**

• **Provide each Admin user with their own user credentials.** User accounts should also only be provided with the permissions vital to job responsibilities.

• **Secure remote access with strong passwords, ensure only the necessary individuals have permission for remote access, disable remote access when not in use, and use two-factor authentication for remote sessions.**

• **Verify the implementation of required security patches**: PCI DSS requires that all system components and software are protected from known vulnerabilities by installing security patches. Visit the PCI SSC website for more information.

• **Monitor network traffic** for suspicious connections, and log system and network events.

• **Implement Network Segmentation**, where possible, to prevent the spread of malicious software and limit an attacker's foothold.

• **Maintain compliance with all security controls defined in the PCI DSS.**

• **In the event of a confirmed or suspected breach, refer to Visa's What to do if Compromised (WTDIC), published October 2019.**

35. Plaintiff believes that Wawa's security flaws run afoul of industry best practices and standards. Specifically, the security practices in place at Wawa during the Data Breach were in direct conflict with the PCI DSS and the 12 PCI DSS core security standards. All merchants are required to adhere to the PCI DSS as members of the payment card industry.

36. As a result of industry warnings, industry practice, the PCI DSS requirements, and multiple well-documented data breaches, Defendants were aware of the risks associated with failing to ensure that their IT systems were adequately secured.

The Wawa Data Breach: the Result of Lax Anti-Virus Standards

37. On or around March 4, 2019, Wawa's payment processing server was breached by a third-party hacker. That hacker took advantage of vulnerabilities in Wawa's point-of-sale system and payment processing servers to install malware that pervasively infiltrated Wawa's systems.

38. The malware "affected customer payment card information used at potentially all Wawa locations" between March 4, 2019 and when the malware was combated by Wawa on December 12, 2019, a full nine months after the initial breach. [6]

[6] An Open Letter from Wawa CEO Chris Gheysens to Our Customers, https://www.wawa.com/alerts/data-security (last accessed Febuary 12, 2020).

39. After discovering the breach on December 10, 2019, Wawa did not contain the breach until December 12, 2019.[7] Wawa failed to inform its customers of the scope of the breach by not publicly announcing the breach until seven days later, on December 19, 2019.

40. The malware installed on Wawa's payment server on or around March 4, 2019 began running on Wawa in-store processing payment systems, including point of sale terminals at both in-store payment terminals and fuel dispenser terminals. Wawa has acknowledged that "this malware was present on most store payment systems by approximately April 22, 2019."[8]

41. The malware successfully collected payment information, including credit and debit card numbers, cardholder names, and expiration dates.[9] Wawa claims "debit card PIN numbers, credit card CVV2 numbers (the three or four-digit security code printed on the card), other PIN numbers, and driver's license information used to verify age-restricted purchases were not affected by this malware."[10] A cybersecurity expert has a acknowledged that CVV numbers are not necessary to create counterfeit copies of the stolen cards.[11] Moreover, other researchers have noted that Track 1 and Track 2 data of the type acknowledged as stolen includes CVV1 numbers.[12]

42. On or around January 27, 2020, approximately 30 million stolen credit card accounts were posted for sale on the popular internet fraud bazaar known as the "Joker's Stash."[13]

---

[7] *See* Wawa Dec. 19, 2019 statement.
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *See* Brian Krebs, *Wawa Security Breach May Have Compromised More Than 30 Million Payment Cards*, https://krebsonsecurity.com/2020/01/wawa-breach-may-have-compromised-more-than-30-million-payment-cards/ (last accessed Feb. 12, 2020).
[12] https://www.nuix.com/blog/howd-they-do-part-2-you-stole-my-credit-card-number (last visited Feb. 12, 2020).
[13] *Id.*

The Joker's Stash noted that the cards were from "a huge new nationwide breach" that purportedly included more than 30 million stolen credit card accounts by thousands of financial institutions across 40 or more U.S. states. This batch of stolen credit cards has been identified on the Joker's Stash as "BIGBADABOOM-III."

43. Gemini Advisory, a New York-based fraud intelligence company noted that the largest concentration of stolen cards for sale in the BIGBADABOOM-III batch map back to Wawa customers in Florida and Pennyslvania.[14] Gemini Advisory also notes that the "median price of US-issued records from this breach is currently $17, with some of the international records priced as high as $210 per card." Further, banks with a nationwide presence and financial institutions along the East Coast "have significant exposure."

44. Defendants failed to maintain and update anti-virus software capable of detecting malware threats despite ongoing and continued hacking at retailers throughout the country. This type of security maintenance is a basic part of running a secure network and protecting card member data.

45. The failure to utilize adequately updated anti-virus and anti-malware systems allowed hackers to infiltrate the POS system such that customer credit and debit card information could be captured.

46. Defendants' IT department and executives were aware that the company was vulnerable to a breach of customer financial information and they were aware of countermeasures on the market which could reduce or eliminate the ability of hackers to steal customer card data

[14] https://geminiadvisory.io/breached-wawa-payment-card-records-reach-dark-web/ (last accessed Feb. 12, 2020).

from POS terminals. Nevertheless, Defendants were negligent in that they failed to adequately protect the credit and debit card data and prevent the Wawa Data Breach.

47. Defendants were not only aware of the threat of data breaches generally, but were aware of the specific danger of malware infiltration. Malware has been used to access POS terminals since at least 2011, and specific types of malware, including RAM scraper malware, have been used recently to infiltrate large retailers such as Target, Sally Beauty, Neiman Marcus, Michaels Stores, and SuperValu. As a result, Defendants were aware that malware is a real threat and is a primary tool of infiltration used by hackers.

48. Defendants received 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 POS malware on July 31, 2014, and issued a guide for retailers on protecting against the threat of POS malware, which was updated on August 27, 2014.[15] Wawa should have taken action to protect and ensure that its customers' information would not continue to be available to hackers and identity thieves, but Wawa chose not to do so.

49. Despite the fact that Defendants were put on notice of the very real possibility of consumer data theft associated with their security practices and despite the fact that Defendants knew or, at the very least, should have known about the basic infirmities associated with the Wawa security systems, they still failed to make necessary changes to their security practices and protocols.

---

[15] *See* United States computer Emergency Readiness Team, *Alert (TA14-212A): Backoff Point-of-Sale Malware* (Aug. 27, 2014), https://www.us-cert.gov/ncas/alerts/TA14-212A (last accessed March 5, 2015).

50. Defendants knew or should have known that failing to protect customer card data would cause harm to the card-issuing institutions such as Plaintiff and the Class because such issuers are financially responsible for fraudulent card activity and must incur significant costs to prevent additional fraud.

51. Defendants, at all times relevant to this action, had a duty to Plaintiff and members of the Class to, and represented that they would:

a. properly secure payment card magnetic stripe information at the point of sale and on Defendants' internal networks;

b. encrypt payment card data using industry standard methods;

c. properly update and maintain anti-virus and anti-malware software;

d. use readily available technology to defend its POS terminals from well-known methods of attack; and

e. act reasonably to prevent the foreseeable harms to Plaintiff and the Class which would naturally result from payment card data theft.

52. Defendants negligently allowed payment card magnetic stripe information to be compromised by failing to take reasonable and prudent steps against an obvious threat.

53. As a direct and proximate result of the events detailed herein, Plaintiff and members of the Class have been injured by, among other things, incurring costs to protect their customers' financial information by cancelling and reissuing cards with new account numbers and magnetic stripe information.

54. The cancellation and reissuance of cards resulted in significant damages and losses to Plaintiff and members of the Class, which were proximately caused by Defendants' negligence.

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

Plaintiff and the Class Have Been Damaged as a Result of Defendants' Wrongdoing

55. Due to Defendants' failure to safeguard customer information, Plaintiff and the class have incurred damages.

56. As a result of the events detailed herein, Plaintiff and members of the proposed Class suffered losses resulting from Wawa's Data Breach related to the need to:

a. cancel or reissue any credit and debit cards affected by the Wawa Data Breach;

b. close any deposit, transaction, checking, or other accounts affected by the Wawa Data Breach, including but not limited to stopping payments or blocking transactions with respect to the accounts;

c. open or reopen any deposit, transaction, checking, or other accounts affected by the Wawa Data Breach;

d. refund or credit any cardholder to cover the cost of any unauthorized transaction relating to the Wawa Data Breach;

e. respond to a higher volume of cardholder complaints, confusion, and concern; and/or

f. increase fraud monitoring efforts.

57. Plaintiff and the class have incurred significant fraud losses. Plaintiff and the class have also incurred internal costs, such as:

a. employee time and overhead charges related to the reissuance of hundreds of cards;

b. providing responses to customer inquiries;

c. notifying customers; and/or

d. dealing with fraudulent charges and crediting its customer's accounts.

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

CHOICE OF LAW

59. The common law of Pennsylvania governs Plaintiff's claims.

60. The principal place of business of Wawa, located in Pennsylvania, is the "nerve center" of its business activities—the place where its high-level officers direct, control, and coordinate the corporation's activities, including its data security functions and major policy, financial, and legal decisions.

61. Pennsylvania has significant interests in regulating the conduct of businesses operating within its borders. Pennsylvania, which seeks to protect the rights and interests of entities against a company headquartered and doing business in that Commonwealth, has a greater interest in the nationwide claims of Plaintiff and Class Members than any other state or commonwealth and is most intimately concerned with the claims and outcome of this litigation.

62. Wawa's response to the Data Breach at issue here, and corporate decisions surrounding such response, were made from and in Pennsylvania.

63. Wawa's breaches of duty owed to Plaintiff and class nembers emanated from Pennsylvania.

64. Application of Pennsylvania law with respect to Plaintiff's and Class Members' claims would be neither arbitrary nor fundamentally unfair because the Commonwealth has

significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiff and Class Members.

65. Under choice of law principles applicable to this action, the common law of Pennsylvania should apply to the nationwide common law claims of all Class Members given the Commonwealth's significant interest in regulating the conduct of businesses operating within its borders. Plaintiff is therefore pleading nationwide claims based upon Pennsylvania law

66. Alternatively, additional factual analysis is necessary in order to determine which state's law should apply to the claims of the Class Members. Accordingly, it would be inappropriate to determine choice of law at the pleadings stage of this case.

CLASS ACTION ALLEGATIONS

67. Plaintiff brings the claims in this action individually and on behalf of all other financial institutions similarly situated nationwide pursuant to Fed. R. Civ. P. 23. The proposed class is defined as:

> All Financial Institutions including, but not limited to, banks and credit unions in the United States (including its Territories and the District of Columbia) that issue payment cards, including credit and debit cards, or perform, facilitate, or support card issuing services, whose customers made purchases from Wawa stores from March 2019 to December 2019 (the "National Class").

Excluded from the National Class are Defendants and their affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff.

68. Plaintiff is a member of the Class it seeks to represent. The Class is so numerous that joinder of all members is impracticable. The members of the Class are readily ascertainable. Plaintiff's claims are typical of the claims of all members of the Class. The conduct of Defendants has caused injury to Plaintiff and members of the Class. Prosecuting separate actions by individual

Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Defendants. Plaintiff will fairly and adequately represent the interests of the Class. Defendants have acted or refused to act on grounds that apply generally to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole. Plaintiff is represented by experienced counsel who are qualified to litigate this case.

69. Common questions of law and fact predominate over individualized questions. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. There are questions of law and fact common to all members of the Class, the answers to which will advance the resolution of the claims of the Class members and that include, without limitation:

a. whether Defendants failed to provide adequate security and/or protection for their computer systems containing customers' financial and personal data;

b. whether the conduct of Defendants resulted in the unauthorized breach of their computer systems containing customers' financial and personal data;

c. whether Defendants failed to properly maintain updated anti-virus and anti-malware systems;

d. whether Defendants' actions were negligent;

e. whether Defendants owed a duty to Plaintiff and the Class;

f. whether the harm to Plaintiff and the Class was foreseeable;

g. whether Plaintiff and members of the Class are entitled to injunctive relief; and

h. whether Plaintiff and members of the Class are entitled to damages and the measure of such damages.

COUNT I
UNFAIR COMPETITION

70. Plaintiff incorporates paragraphs 1-58 as if fully set forth herein.

71. Defendants caused harm to the commercial relations of Plaintiff and the Class Members and their customers.

72. Defendants, in the normal course of its business, collected customer information, including debit and credit card information and PII.

73. Defendants failed to properly implement adequate, commercially reasonable security measures to protect customers' debit and credit card information and PII, by failing to warn shoppers that their information was at risk, and by failing to immediately notify affected customers of the nature and extent of the security breach.

74. Defendants caused harm to Plaintiff and Class Members by, among other things, misrepresenting the safety and security of their payment systems through deceptive marketing and unfair methods of competition.

75. Plaintiff and the other members of the Class have suffered injury in fact and substantial losses as detailed herein, including lost money and property, as a result of Defendants' unfair competition.

COUNT II
NEGLIGENCE

76. Plaintiff incorporates and re-alleges paragraphs 1-58 as if fully set forth herein.

77. Defendants owed a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining and processing Plaintiff's customers' personal and financial information.

78. Defendants owed a duty to Plaintiff and the Class to provide adequate security to protect their mutual customers' personal and financial information.

79. Defendants breached their duties by (1) allowing a third-party intrusion into their computer systems; (2) failing to protect against such an intrusion; (3) failing to maintain updated anti-virus and anti-malware software necessary to prevent such an intrusion; and (4) allowing the personal and financial information of customers of Plaintiff and the Class to be accessed by third parties on a large scale.

80. Defendants knew or should have known of the risk that their POS terminals could be infiltrated using methods similar or identical to those previously used against major retailers in recent months and years.

81. Defendants knew or should have known that their failure to take reasonable measures to protect their POS terminals against obvious risks would result in harm to Plaintiff and the Class.

82. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and the Class have suffered substantial losses as detailed herein.

COUNT III
NEGLIGENCE *PER SE*

83. Plaintiff incorporates and re-alleges paragraphs 1-58 as if fully set forth herein.

84. Through their acceptance of credit and debit payment cards and participation in the payment card processing system at Wawa stores, Defendants held themselves out to Plaintiff and the Class as possessing and maintaining adequate data security measures and systems that were sufficient to protect the personal and financial information of shoppers using credit and debit cards issued by Plaintiff and the Class.

85. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair…practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice the unfair practice of failing to use reasonable measures to protect PII by retailers such as Wawa. The FTC publications described above also form the basis of Defendants' duty.

86. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measure to protect PII and not complying with applicable industry standards, including PCI DSS as described in detail previously in this complaint. Defendants' conduct was particularly unreasonable given the amount of PII it obtained and stored and the foreseeable consequences of a data breach at a fuel dispenser chain, including specifically the immense damages that would result to consumers and financial institutions.

87. Wawa's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

88. The Financial Instituition Plaintiff and class are within the class of persons Section 5 of the FTC Act was intended to protect as they are engaged in commerce and bear primary responsibility for reimbursing consumers for fraud losses. Moreover, the named Plaintiff and many absent Class Members are credit unions, which are organized as cooperatives whose members are consumers.

89. Moreover, the harm that has occurred is the type of harm the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions business which, as a result of their failure to employ reasonable data security measures, caused the same harm suffered by the Class.

90. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT IV
DECLARATORY AND INJUNCTIVE RELIEF

91. Plaintiff incorporate and re-alleges paragraphs 1-58 as if fully set forth herein.

92. 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 based upon such a judgment. 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 in this complaint.

93. An actual controversy has arisen in the wake of Defendants' data breach regarding its common law and other duties to reasonably safeguard its customers' PII. Defendants allege that their security measures were adequate and remain adequate. Plaintiff and the Class deny these allegations. Furthermore, Plaintiff and the Class continue to suffer injury as additional fraudulent charges continue to be made on payment cards they issued to Defendants' customers.

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

a. Defendants owed and continue to owe a legal duty to secure their customers' personal and financial information, including specifically information pertaining to credit and debits cards used by Defendants' customers, under the common law, Section 5 of the FTC Act, its contracts with payment processors, Card Operating Regulations issued by card networks, PSI DSS standards, and various state statutes;

b. Defendants breached and continue to breach this legal duty by failing to employ reasonable measure to secure their customers' personal and financial information;

c. Defendants' breach of its legal duty proximately caused the data breach which occurred between March and December 2019; and,

d. Banks, credit unions, and other institutions that reissued payment cards and were forced to pay for fraudulent transactions as a result of the Defendants' data breach are legally entitled to recover the costs they incurred from Defendants.

95. The Court also should issue corresponding injunctive relief requiring Defendants to employ adequate security protocols consistent with industry rules and standards to protect its customers' personal and financial information. Specifically, this injunction should, among other things, direct Defendants to do the following :

- utilize industry standard encryption to encrypt transmission of cardholder data and sensitive information at the point-of-sale and at all other times;
- implement encryption keys in accordance with industry standards;
- consistent with industry standards, engage third party security auditors to test its systems for weakness and upgrade any such weakness found;
- audit, test, and train its security personnel regarding any new or modified procedures and how to respond to a security breach;
- regularly test its systems for security vulnerabilities, consistent with industry standards;
- comply with all PCI DSS standards pertaining to the security of its customers' personal and confidential information;
- install in a timely manner all upgrades recommended by manufacturers of security software and firewalls used by Defendants; and

- delete its customers' credit card information immediately after obtaining authorization to process the transaction and debit card information.

96. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Defendants' locations. The risk of another such breach is real, immediate, and substantial. If another breach at Defendants' locations occurs, Plaintiff and the Class 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.

97. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another massive data breach occurs at Defendants' locations, Plaintiff and the Class will likely incur hundreds of millions of dollars in damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable data security measures is relatively minimal.

98. 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 Defendants' locations, thus eliminating the injuries that would result to Plaintiff and the Class and the millions of consumers whose confidential information would be compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that this Court enter a judgment against Defendants and in favor of Plaintiff and the Class and award the following relief:

A. That this action be certified as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, declaring Plaintiff as representative of the Class and Plaintiff's counsel as counsel for the Class;

B. Monetary damages, including punitive damages;

C. Injunctive relief;

D. Reasonable attorneys' fees and expenses, including those related to experts and consultants;

E. Costs;

F. Pre- and post-judgment interest; and

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

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Plaintiff, individually and on behalf of the Class, demands a trial by jury for all issues so triable.

DATED: February 18, 2020

Respectfully submitted,

/s/ Jeannine M. Kenney
Jeannine M. Kenney
HAUSFELD LLP
325 Chestnut St #900
Philadelphia, PA 19106
(215) 985-3270
jkenney@hausfeld.com

James J. Pizzirusso
HAUSFELD LLP
1700 K Street, NW
Suite 650
Washington, DC 20006
(202) 540-7200
jpizzirusso@hausfeld.com

Mindee J. Reuben
LITE DEPALMA GREENBERG, LLC
1835 Market Street
Suite 2700
Philadelphia, PA 19103
(267) 314-7980

mreuben@litedepalma.com

Joseph D. DePalma
Jeremy N. Nash
LITE DEPALMA GREENBERG, LLC
570 Broad Street
Suite 1201
Newark, NJ 07102
(973) 623-3000
jdepalma@litedepalma.com
jnash@litedepalma.com

Amy E. Keller
DICELLO LEVITT GUTZLER LLC
Ten North Dearborn Street, Eleventh Floor
Chicago, Illinois 60602
(312) 214-7900
akeller@dicellolevitt.com

Arthur N. Bailey
Marco Cercone
R. Anthony Rupp, III
RUPP BAASE PFALZGRAF CUNNINGHAM LLC
1600 Liberty Building
424 Main Street
Buffalo, New York 14202
(716) 854-3400
bailey@ruppbaase.com
cercone@ruppbaase.com
rupp@ruppbaase.com

Attorneys for Plaintiff and the Putative Class

JS 44 (Rev. 02/19)

CIVIL COVER SHEET

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.)*

I. (a) PLAINTIFFS

Greater Chautauqua Federal Credit Union

(b) County of Residence of First Listed Plaintiff Chautauqua County
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Jeannine M. Kenney, Hausfeld LLP, 325 Chestnut St. #900, Philadelphia, PA 19106, (215) 985-3270
Mindee Reuben, Lite Depalma Greenburg, 1835 Market, 267-314-7980

DEFENDANTS

Wawa Inc. and Wild Goose Holding Co., Inc.

County of Residence of First Listed Defendant Delaware County
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*
Ezra Dodd Church & Gregory Parks, Morgan Lewis & Bockus, 1701 Market St., Philadelphia, PA, (215) 963-5710

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

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

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

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

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

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

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

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

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

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. Section 1332(d)

Brief description of cause:
Action in diversity to recover damages cause by Defendants negligence, negligence per se, and unfair competition

VII. REQUESTED IN COMPLAINT:

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

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE Hon. Gene E. K. Pratter DOCKET NUMBER 19-cv-6019

DATE 02/18/2020

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

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: Greater Chautauqua Fed. Credit Union, 51 East Main Street, Falconer, New York

Address of Defendant: Wawa, Inc. & Wild Goose Holding Co., 260 W. Baltimore Pike, Media, PA 19063

Place of Accident, Incident or Transaction: Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida, District of Columbia

RELATED CASE, IF ANY:

Case Number: 19-cv-6019 Judge: Hon. Gene E. K. Pratter Date Terminated: _____

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

		Yes	No
1.	Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court?	☐	☑
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?	☑	☐
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?	☐	☑
4.	Is this case a second or successive habeas corpus, social security appeal, or pro se civil rights case filed by the same individual?	☐	☑

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: 02/18/2020 Must Sign Here _____ 307635
Attorney-at-Law / Pro Se Plaintiff *Attorney I.D. # (if applicable)*

CIVIL: (Place a √ in one category only)

A.	***Federal Question Cases:***	*B.*	***Diversity Jurisdiction Cases:***
☐	1. Indemnity Contract, Marine Contract, and All Other Contracts	☐	1. Insurance Contract and Other Contracts
☐	2. FELA	☐	2. Airplane Personal Injury
☐	3. Jones Act-Personal Injury	☐	3. Assault, Defamation
☐	4. Antitrust	☐	4. Marine Personal Injury
☐	5. Patent	☐	5. Motor Vehicle Personal Injury
☐	6. Labor-Management Relations	☐	6. Other Personal Injury *(Please specify):* _____
☐	7. Civil Rights	☐	7. Products Liability
☐	8. Habeas Corpus	☐	8. Products Liability – Asbestos
☐	9. Securities Act(s) Cases	☑	9. All other Diversity Cases
☐	10. Social Security Review Cases		*(Please specify):* 28 U.S.C. Section 1332(d)
☐	11. All other Federal Question Cases		
	(Please specify): _____		

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

I, Jeannine M. Kenney, 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: 02/18/2020 Sign Here if Applicable _____ 307635
Attorney-at-Law / Pro Se Plaintiff *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)

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

CASE MANAGEMENT TRACK DESIGNATION FORM

Greater Chautauqua Federal Credit Union, individually and on behalf of a class similarly situated	CIVIL ACTION
v.	
Wawa Inc. and Wild Goose Holding Co., 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. ( )

February 18, 2020	Jeannine M. Kenney	Greater Chautauqua Federal Credit Union,
Date	**Attorney-at-law**	**Attorney for**
215-985-3270	215-985-3271	jkenney@hausfeld.com
Telephone	**FAX Number**	**E-Mail Address**

(Civ. 660) 10/02