

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA**

INSIGHT CREDIT UNION, on Behalf of)	Civil Case No.
Itself and All Others Similarly Situated,)	
)	CLASS ACTION COMPLAINT
Plaintiff,)	
)	JURY TRIAL DEMANDED
v.)	
)	
WAWA, INC.)	
)	
Defendant.)	
)	
)	

INTRODUCTION

1. Wawa, Inc. (“Wawa”), a privately-owned company operating over 850 gas stations and convenience stores, has allowed one of the largest and longest payment card data breaches in history, resulting in an estimated 30 million compromised payment cards (“Data Breach”).
2. Wawa is one of the nation’s largest private companies with over 37,000 employees. Wawa’s 850 stores serve approximately 800 million customers annually, and rakes in over \$12 billion annually. Its stores are concentrated in 6 states – Pennsylvania, Florida, Delaware, Maryland, New Jersey, Virginia – and the District of Columbia.
3. Despite Wawa’s substantial annual revenue and relatively few stores, Wawa utterly failed to implement reasonable, standard, and required data security measures necessary to protect the payment information of its hundreds of millions of customers. Indeed, during the Data Breach data security experts and Wawa’s own personnel estimate that hackers successfully placed card-stealing malware *at every single* Wawa store.
4. After failing to prevent hackers from intruding into its stores, Wawa similarly failed to timely detect its Data Breach. During the Data Breach, the hackers had near unfettered access

into Wawa's POS systems for over nine months. While the Data Breach began on March 4, 2019 Wawa admitted that all of its over 850 convenience stores and gas stations had likely been compromised by April 22, 2019.

5. Wawa only identified the Data Breach on December 10, 2019, allegedly containing the breach two days later. However, the damage was already done – tens of millions of payment cards had been stolen by hackers during eight months of unrestricted access to customer payment card data at all of Wawa's stores.

6. Wawa admitted it failed its customers. In an Open Letter announcing the Data Breach, Wawa stated that it “ha[d] experienced a data security incident” and “malware on Wawa payment processing servers . . . affected customer payment card information used at potentially all Wawa locations”¹

7. Highlighting the significant scope of the Data Breach, on January 27, 2020, the website Joker's Stash, a notorious site on the dark web that facilitates the sale of stolen payment cards, posted an announcement of “Brand NEW Huge 30M+ pcs Nationwide[,]” calling the massive payment card data dump “BIGBADABOOM-III.”² The post indicated the stolen cards would be available the evening of January 27, 2020.

8. KrebsOnSecurity, a well-known data security blog, reported that “[t]wo sources that work closely with financial institutions nationwide . . . that the new batch of cards that went

¹ *Notice of Data Breach*, Wawa.com/alerts/data security (last visited Jan. 31, 2020), <https://www.wawa.com/alerts/data-security>

² Brian Krebs, *Wawa Breach May Have Compromised More than 30 Million Payment Cards*, KrebsOnSecurity (Jan. 28, 2020), <https://krebsonsecurity.com/2020/01/wawa-breach-may-have-compromised-more-than-30-million-payment-cards/>

on sale . . . [were] ma[ped] squarely back to cardholder purchase at Wawa.”³ Similarly, Gemini Advisory, a New York-based fraud intelligence company, said the biggest concentration of stolen cards for sale in the BIGBADABOOM-III batch were linked to Wawa customer cards used in Florida and Pennsylvania, the two states with the most Wawa stores.⁴

9. Wawa’s Data Breach should not have happened. Wawa knew of data security measures capable of preventing or limiting the scope of a data breach involving POS systems. For example, Wawa, because it accepted payment cards, was obligated to adhere to certain data security requirements set forth in the Payment Card Industry Data Security Standards (“PCI DSS”). PCI DSS was created by the Payment Card Industry, including Visa, MasterCard, American Express, Discover and JCB International (the “Card Brands”), to provide “technical and operational requirements . . . to protect card holder data” that applied to “all merchants organizations that store, process or transmit [payment card] data . . .”⁵ Because, at all relevant times, Wawa processed payment card data, it was obligated by its agreements with the Card Brands to comply with PCI DSS.

10. In addition to PCI DSS compliance, the Federal Trade Commission (“FTC”), state governments, and data security organizations created industry standards and made recommendations designed to prevent and limit the scope of a data breach. Generally, these measures are more rigorous than the PCI DSS. One such standard, for example, was the ISO/IEC

³ *Id.*

⁴ Alforov, Stas & Thomas, Christopher, *Breached Wawa Payment Card Records Reach Dark Web*, Gemini Advisory (Jan. 28, 2020), <https://geminiadvisory.io/breached-wawa-payment-card-records-reach-dark-web/>

⁵ *Payment Card Industry Security Standards*, PCI SECURITY STANDARDS COUNCIL (Oct. 2010), https://www.pcisecuritystandards.org/documents/PCI_SSC_Overview.pdf?agreement=true&time=1560370308360

27000 information security management system standard published by the International Organization for Standardization and the International Electrotechnical Commission. ISO/IEC 27000 was designed to provide standard best practices for implementing a comprehensive data security program, including implementing adequate security tools, security personnel, and security departments and creating a sufficient data security response program. Many data security analysts refer to these best practices when assessing a company's data security posture.

11. Moreover, the FTC has also made it clear to companies accepting payment card data that the failure to take reasonable security measures to protect the security and confidentiality of such data constitutes a violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. §45, and will be fined accordingly. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 613 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015); *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act); *In re BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148, FTC File No. 042-3160 (Sept. 20, 2005) (same); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC File No. 052-3148 (Sept. 5, 2006) (same); *see also United States v. ChoicePoint, Inc.*, Civil Action No. 1:06-cv-0198-JTC (N.D. Ga. Oct. 14, 2009) (“failure to establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers” violates § 5(a) of FTC Act); 15 U.S.C. §45(n) (defining “unfair acts or practices” as those that “cause[] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”).

12. Given the highly publicized data breaches that have occurred over the past five years, the PCI DSS, the data security best practices set forth by other independent organizations, and the FTC's approach to data security, Wawa fully knew its POS systems would be a target for hackers, understood the vulnerabilities of its POS systems, and understood that, if not resolved, those vulnerabilities increased the likelihood of a data breach. Wawa also knew of reasonable data security measures that would prevent hackers from infiltrating its systems, prevent the application of malware on its POS systems, and allow for fast identification and remediation of any intrusion.

13. As a result of Wawa's Data Breach, Plaintiff and the Class received alerts notifying them that their payment card accounts were compromised. In response, Plaintiff and the Class took measures to prevent further harm, including: (a) canceling or reissuing credit and debit cards affected by Wawa's Data Breach; (b) closing deposit, transaction, checking, or other accounts affected by Wawa's Data Breach, including, but not limited to, stopping payments or blocking transactions with respect to the accounts; (c) opening or reopening deposit, transaction, checking, or other accounts affected by Wawa's Data Breach; (d) refunding credit card holders to cover the cost of unauthorized transactions relating to Wawa's Data Breach; (e) responding to a higher volume of cardholder complaints, confusion, and concern; and/or (f) increasing fraud monitoring efforts. These measures, taken by Plaintiff, caused it substantial damages.

14. Ironically, in its Open Letter, Wawa wrote: "I want to reassure you that you will not be responsible for any fraudulent charges on your payment cards related to this incident"⁶ Wawa failed to mention, however, that *it* would not be responsible for paying the fraudulent charges on customers' payment cards. Rather, financial institutions carry that burden. Indeed, reports from financial institutions state that in the wake of Wawa's Data Breach, financial

⁶ *Notice of Data Breach, supra* note 1.

institutions replaced their payment card data in droves to prevent the misuse of payment cards stolen during the Data Breach.⁷

15. As alleged herein, the injuries to Plaintiffs and the Class were directly and proximately caused by Wawa's failure to implement and maintain adequate and reasonable data security measures necessary for protecting customer information, including credit and debit card data. Wawa failed to take steps to employ adequate security measures despite well-publicized data breaches at large national retail and restaurant chains in the months and years preceding the Data Breach, including Target, Home Depot, P.F. Chang's, Eddie Bauer, Wendy's, Dairy Queen, Noodles & Co., Arby's, Chipotle, Kmart and Sonic.

16. This class action is brought on behalf of financial institutions throughout the United States to recover the costs that they have been forced to bear as a direct result of the Data Breach of Wawa's systems and to obtain other equitable relief. Plaintiff asserts claims for negligence, negligence per se, violations of Florida's Unfair and Deceptive Practices Act, and for declaratory and injunctive relief.

JURISDICTION AND VENUE

17. This Court has original jurisdiction of this Action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332 (d)(2). The matter in controversy, exclusive of interest and costs, exceeds the sum or value of \$5,000,000 and at least some members of the proposed Class have a different citizenship than Wawa.

18. This Court has personal jurisdiction over Wawa because Wawa maintains its principal place of business in Wawa, Pennsylvania, regularly conducts business in Pennsylvania,

⁷ Christian Hetrick, *After Wawa breach, banks reissue thousands of debit, credit cards to customers*, Philadelphia Inquirer (Jan. 3, 2020), <https://www.inquirer.com/news/wawa-citibank-citizens-bank-credit-debit-breach-hack-20200103.html>

and has sufficient minimum contacts in Pennsylvania. Wawa intentionally availed itself of this jurisdiction by accepting and processing payments for its services and goods within Pennsylvania.

19. Venue is proper under 18 U.S.C. § 1391(a) because Wawa's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

20. **Plaintiff** Insight Credit Union is a Florida-chartered credit union with its principal place of business located in Orlando, Florida. Plaintiff received notice that payment cards it issued to its members had been compromised in the Wawa Data Breach, and Plaintiff took action in response to minimize the impact to its members and its institution. As a result of the Wawa Data Breach, Plaintiff has suffered injury, including, *inter alia*, costs to cancel and reissue cards, costs to refund fraudulent charges, and costs to investigate and monitor impacted cards, among other losses.

21. **Defendant** Wawa, Inc. maintains its headquarters at 260 West Baltimore Pike, Wawa, Pennsylvania 19063. Wawa is a privately held company that owns and operates over 850 convenient stores and gas stations located along the east coast in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida, and Washington, D.C. Reports indicate that Wawa stores serve roughly 800 million customers annually.

ALLEGATIONS

22. Wawa describes itself as “your all-day, everyday convenience store with breakfast, lunch, and dinner, Built-To-Order foods and beverages, coffee, fuel, and much more.”⁸ It owns and operates over 850 gas stations and convenience stores in Pennsylvania, Florida, Delaware,

⁸ *About*, Wawa.com (last visited, Jan. 31, 2020), <https://www.wawa.com/about>

Maryland, New Jersey, Virginia, and the District of Columbia.⁹ New Jersey, Pennsylvania, and Florida are home to over 75% of Wawa's stores.¹⁰

23. Wawa serves approximately 800 million customers annually and each year, exceeds \$12 billion in gross revenue.¹¹ In all, Wawa is one of the nation's largest private companies with over 37,000 employees.

24. Wawa claims to value its customers, writing "nothing is more important than honoring and protecting [our customers'] trust" and that customers are its customers are Wawa's "top priority and are critically important to all of the nearly 37,000 associates at Wawa."¹² Wawa further claims to take its "special relationship with [its customers] and the protection of [its customers'] information very seriously."¹³

25. Wawa's official Privacy Policy states:

Protecting your privacy is important to Wawa. This Wawa Privacy Policy ('Policy') describes how Wawa and its subsidiaries and affiliated companies collect, use, disclose and safeguard the personal information you provide on Wawa's websites, www.wawa.com and www.wawarewards.com, and through or in connection with our mobile apps or other software- and Internet-enabled programs and services sponsored by Wawa (the "Sites") as well as information collected when you visit our stores or otherwise communicate or interact with Wawa.¹⁴

⁹ *Id.*

¹⁰ Alforov & Thomas, *supra* note 4.

¹¹ *America's Largest Private Companies*, Forbes.com (last visited, Jan. 31, 2020), https://www.forbes.com/largest-private-companies/list/#tab:rank_search:wawa

¹² *Notice of Data Breach*, *supra* note 1.

¹³ *Id.*

¹⁴ *Wawa Official Privacy Policy*, Wawa.com (last visited, Jan. 31, 2020), <https://www.wawa.com/privacy>.

26. Despite its policies and proclamations, Wawa did not prioritize protecting customer information. Rather, its deficient data security measures left the payment card information for every single one of its customers from March 4, 2019 to December 12, 2019 at all of its stores and gas stations vulnerable to theft.

27. On December 19, 2019, Wawa acknowledged that it had suffered a massive Data Breach spanning nine months and affecting all of its restaurants.¹⁵ As a result, little more than a month later, hackers posted over 30 million payment cards on Joker's Stash, a website used to sell stolen payment cards to fraudsters.¹⁶

28. Wawa sought to downplay the extent of harm to consumers by writing: "I want to reassure you that you will not be responsible for any fraudulent charges on your payment cards related to this incident."¹⁷

29. Wawa was right, its customers will not be responsible for the fraudulent charges on their payment cards caused by Wawa's Data Breach. But Wawa will also not carry the lion's share of that burden. Rather, the financial institutions who issued the compromised payment cards will be forced to pay the fraudulent charges, in addition to card replacement and other damages, directly attributable to Wawa's inadequate data security measures and Data Breach.

30. Wawa acknowledges, in part, this fact, writing to its customers: "Under federal law and card company rules, customers who notify their payment card issue in a timely manner of fraudulent charges will not be responsible for those charges."¹⁸

¹⁵ *Notice of Data Breach*, *supra* note 1.

¹⁶ Krebs, *supra* note 2.

¹⁷ *Notice of Data Breach*, *supra* note 1.

¹⁸ *Id.*

31. Thus, as a result of Wawa's negligent data security measures and its massive (in both scope and length) Data Breach, financial institutions will suffer significant harm. Had Wawa implemented reasonable well-known, recommended, and often required data security measures, it could have prevented the Data Breach. It failed to do so.

Wawa Was On-Notice of the Vulnerabilities of Point-of-Sale ("POS") Systems

32. POS systems provide the hardware, software, and networks responsible for facilitating payments made by credit and debit cards. At a POS terminal, "data contained in [a payment] card's magnetic stripe is read and then passed through a variety of systems and networks before reaching the retailer's payment processor."¹⁹ The payment processor completes the transaction by passing payment information to the appropriate Card Brand (Visa, MasterCard, etc.) networks and then to the financial institution that issued the card for approval of the transaction.²⁰ Once approved, the retailer is paid by an acquiring or merchant bank, and the issuing bank later reimburses the acquiring bank for the transaction.

33. To send payment card information to the payment processor, businesses use a Cardholder Data Environment, usually referred to as a CDE or a CHDE.²¹ The CDE is a part of the POS system and represents the network that transfers card information from the POS terminal to the payment processor who assists with authorizing the transactions. Elements of the CDE include all network components like firewalls, switches, routers, access points, and network

¹⁹ Symantec, *A Special Report On Attacks On Point-of-Sale Systems* 6 (Nov. 20, 2014), <https://www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf>.

²⁰ Slava Gomzin, *Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions* 8 (Wiley 2011).

²¹ *Id.* at 39.

appliances, POS systems, servers, and often virtual components like virtual machines, switches, routers, desktops and hypervisors.²²

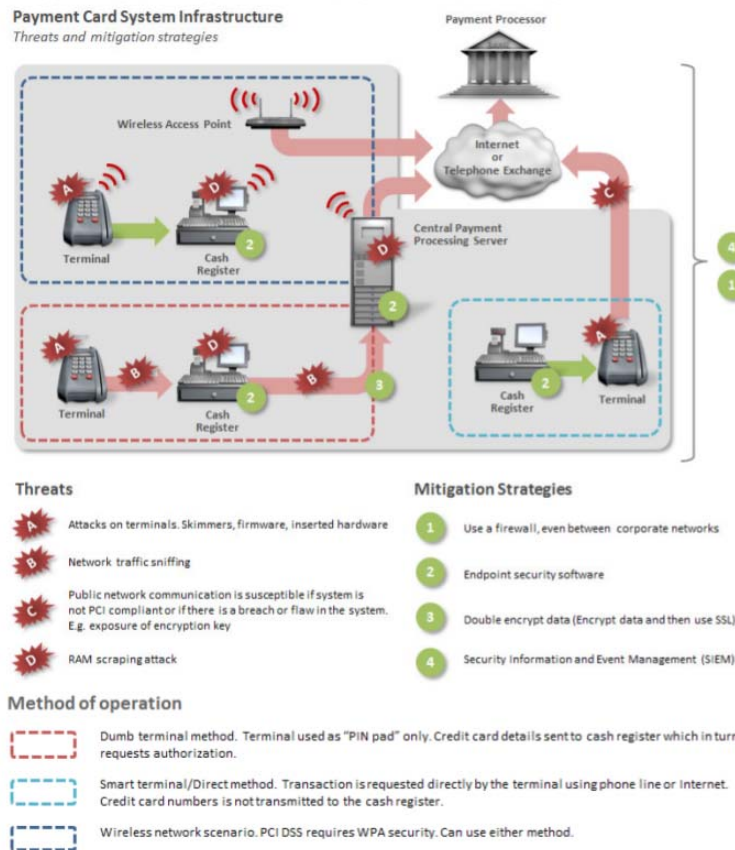


Figure 1. An example of a CDE and its vulnerabilities.

34. When hackers gain access to POS systems, they have direct access to payment card information. Before transmitting consumer purchasing information over the network through the deployment architecture, the POS system typically, very briefly, stores data from the card's magnetic stripe in unencrypted plain text within the POS system's memory before transfer or

²² *Cardholder Data Environment (CDE)*, TechTarget.com (last visited, Jan. 2, 2019) (noting "[m]ost data breaches in the retail sector involve a compromise of the cardholder data network."), <https://searchsecurity.techtarget.com/definition/cardholder-data-environment-CDE>

encryption.²³ Stored payment information includes “Track 1” and “Track 2” data—originally stored on the magnetic stripe of the payment card—which includes the full information about the cardholder, including first and last name, the expiration date of the card, and the CVV (three number security code on the card).²⁴ This information is unencrypted on the card and, if left unencrypted on the POS device, is easily accessible by hackers using common malware.²⁵ Hackers with access to Track 1 and Track 2 payment card data can physically replicate the card for in person use or can use the data to make fraudulent purchases online.

35. To gain access to POS systems, hackers generally use four general steps: incursion, discovery, capture, and exfiltration.²⁶ In the incursion phase, an attacker gains access to the targeted environment, which normally includes hacking into a business’s corporate network and finding an entry point into the CDE. To access the corporate network, hackers often use phishing attacks which “trick[] or bait[] employees into giving access to the company’s network.”²⁷ Phishing emails seek to fool employees into opening malicious attachments or unknowingly providing their login information to the nefarious actors.

36. In the second phase, the attacker escalates his privileges and explores the systems to learn about its security measures and where the targeted data is located. Using employee credentials gained in a phishing attack, the hackers find vulnerabilities in the corporate network or

²³ Symantec, *supra* note 19, at 6.

²⁴ Gomzin, *supra* note 20, at 98-101.

²⁵ Symantec, *supra* note 19, at 5.

²⁶ *Id.* at 4.

²⁷ Trend Micro, *Data Breaches 101: How They Happen, What Gets Stolen, and Where it Goes*, Trendmicro.com (Aug. 10, 2018), <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101>

attempt to obtain administrative privileges to obtain access to the CDE. The CDE provides access to the physical POS machines at in-store locations, and therefore, once a hacker breaches the CDE, the hacker may access the POS systems and terminals at in-store locations.²⁸

37. In the third phase, the hackers collect the targeted data. In POS data breaches, the malware is almost always a card-scraping malware that steals payment card data directly off of the POS systems and aggregates that data for exfiltration.

38. In the fourth phase, the captured data is placed at an aggregation point and is transferred to a system outside the target environment where it can be retrieved and used for whatever nefarious purposes the cybercriminal intended.²⁹ Often, the hackers attempt to monetize the stolen data and, in the case of POS data breaches, sell payment card data to fraudsters.

39. According to one report, “[t]he vast majority of successful breaches leverage legitimate credentials to gain access to the POS environment. Once attackers gain access to the POS devices, they install malware, usually a RAM scraper, to capture payment card data.”³⁰ Hackers, on average, successfully compromise unsecured POS systems in a matter of minutes or hours and exfiltrated data within days of placing malware on the POS devices.³¹

40. Wawa knew or should have known hackers would target its POS systems to obtain customer payment card information. Since 2013, malware installed on POS systems has been responsible for nearly every major data breach of a retail outlet or chain restaurant. In 2015 alone,

²⁸ Symantec, *supra* note 19, at 6.

²⁹ *Id.*

³⁰ *2016 Data Breach Investigations Report*, Verizon at 1 (Apr. 2016), http://www.verizonenterprise.com/resources/reports/rp_2016-DBIR-Retail-Data-Security_en_xg.pdf

³¹ *Id.* at 4.

data breaches into POS systems accounted for 64% of *all* breaches where hackers successfully stole data.³² In 2014, retail entities replaced credit, banking and financial institutions as the leader in greatest number of data breaches experienced per year and by far, the most common means of data theft is through hacking, phishing, or skimming schemes targeting POS systems.³³

41. These breaches have resulted in hundreds of millions of compromised payment cards,³⁴ and the number of breaches has continued to increase.³⁵ Since the 2014 Target Data Breach, the media has reported data breaches at numerous businesses and other chain restaurants, including: Neiman Marcus, Michaels, Sally Beauty Supply, P.F. Chang's China Bistro, Eddie Bauer, Goodwill, SuperValu Grocery, UPS, Home Depot, Jimmy John's, Dairy Queen Restaurants, Staples, Kmart, Noodles & Co., GameStop, Wendy's, Chipotle and Arby's, among others. These breaches have been well publicized and most or all involved RAM scraping POS malware similar to that employed in the Wawa Data Breach. Given the numerous, well-publicized retail outlet and fast-food data breaches, Wawa was on notice that its POS systems would be targeted and a breach could lead to the theft of millions of customers' payment card information.

42. Additionally, data security experts have specifically and publicly warned businesses, like Wawa, about the threats of data breaches at gas stations. In 2019, Visa warned that gas stations were emerging as a primary target for cybercriminals because gas stations were

³² *Id.* at 3.

³³ *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScourt*, Identity Theft Resource Center (Jan. 19, 2017), <http://www.idtheftcenter.org/2016data-breaches.html>.

³⁴ Symantec, *supra* note **Error! Bookmark not defined.**, at 3.

³⁵ *See* Identity Theft Resource Center, *supra* note 33.

slow to adopt secure payment processing technology, including EMV.³⁶ EMV, which has been available for years, uses a computer chip to provide dynamic credit card information that cannot be duplicated in later fraudulent charges. EMV replaces the long-standing magnetic strips at the back of payment cards that use static payment card information capable of being duplicated and reused by criminals for nefarious purposes. Visa similarly warned of multiple alleged security incidents at gas stations in 2019, and that gas station attacks were increasing in frequency and sophistication.³⁷

43. Additionally, experts have long-warned that “the threat is serious. Beyond POS systems, fraudsters often go directly to the source by attacking the restaurant’s network or computer system, which stores files containing sensitive financial details. POS network attacks can affect multiple chain locations simultaneously and expose immense quantities of data in one fell swoop, allowing attackers to remotely steal data from each credit card as it is swiped at the cash register.”³⁸ However, these data breaches are preventable: “To help prevent fraud attacks, restaurants need to ensure they comply with the standards governing the handling of payment card information, . . . manage the risks associated with third party vendors and put an effective incident response plan into place.”³⁹

³⁶ Visa Security Alert, *Attacks Targeting Point-of-Sale at Fuel Dispenser Merchants*, Visa.com (last visited, Jan. 31, 2020), <https://usa.visa.com/dam/VCOM/global/support-legal/documents/visa-security-alert-attacks-targeting-fuel-dispenser-merchant-pos.pdf>.

³⁷ Jai Vijayan, *Visa Warns of Targeted PoS Attacks on Gas Station Merchants*, Dark Reading (Dec. 13, 2019), <https://www.darkreading.com/attacks-breaches/visa-warns-of-targeted-pos-attacks-on-gas-station-merchants/d/d-id/1336619>.

³⁸ Michael Reiblat, *Is your restaurant data-breach proof?*, Fast Casual (Aug. 3, 2018), <https://www.fastcasual.com/blogs/is-your-restaurant-data-breach-proof>.

³⁹ *Id.*

44. These warnings, among others, put Wawa on notice that it may be susceptible to a data breach and of the importance of prioritizing data security to prevent a breach. Despite Wawa's knowledge of the likelihood that its customers' payment card information would be stolen without reasonable security measures, and that its CDE and POS systems were a target of hackers, Wawa implemented woefully inadequate data security measures that allowed hackers to easily penetrate its systems and steal payment card information.

***Hackers Accessed Wawa's Point-of-Sale Systems
Due to Its Unreasonable Security Measures***

45. Wawa is, and at all relevant times was, aware that the payment card data it receives via credit and debit card transactions is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases. Wawa knew of the necessity of safeguarding payment card data and of the foreseeable consequences that would occur if its data security systems were breached, including the significant costs that would be imposed on issuers, such as the Plaintiff and members of the Class. Numerous widely reported data breaches put Wawa on notice of the means by which hackers infiltrate POS systems and obtain payment card data.

46. Wawa is, and at all relevant times was, fully aware of the significant volume of daily credit and debit card transactions at Wawa's convenience stores and gas stations, amounting to tens of thousands of daily credit card transactions and hundreds of millions of annual customers. Thus, Wawa understood a significant number of individuals and businesses would be harmed by a breach of Wawa's payment systems.

47. Despite this knowledge, Wawa woefully failed to protect its customers' payment card data, allowing hackers to infiltrate its CDE and the POS devices at every single one of its over 850 stores and gas stations. During a nine-month long Data Breach, hackers collected tens

of millions of customer payment cards, eventually publishing those cards to dark web and selling them to fraudsters.

48. The Wawa Data Breach became public on December 19, 2019, when Wawa posted an Open Letter on their website notifying customers of the Data Breach. Wawa wrote that:

Our information security team discovered malware on Wawa payment processing servers on December 10, 2019, and contained it by December 12, 2019. This malware affected customer payment card information used at potentially all Wawa locations beginning at different points in time after March 4, 2019 and until it was contained. At this time, we believe this malware no longer poses a risk to Wawa customers using payment cards at Wawa, and this malware never posed a risk to our ATM cash machines.⁴⁰

...

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

49. The substantial scope and length of the Wawa Data Breach indicates Wawa's data security measures were woefully deficient. Indeed, Ron Schlecht, a data security expert at BTB Security wrote: "What is most shocking to me, and should be most appalling to everybody, is how long this went undetected. How did Wawa just find this recently? They were obviously not monitoring at an appropriate level commensurate with their business volume and were unable to detect this anomalous activity."⁴¹

⁴⁰ *Notice of Data Breach*, *supra* note 1.

⁴¹ Christian Hetrick, 'They wre obviously not monitoring at an appropriate level'' *Before Wawa data breach, Visa warned it could happen*, Morning Call (Jan. 2, 2020), <https://www.mcall.com/news/pennsylvania/mc-nws-pa-wawa-data-breach-20200102-sp2mm3eulneqhe6d7vbw56byse-story.html>.

50. Wawa's data security measures must have failed at multiple levels for the Data Breach to have occurred and continued for months unnoticed. Basic data security practices that Wawa lacked have been recommended for years and required by the PCI DSS and other well-known data security standards. These measures are intended to prevent a data security incident or quickly identify and resolve an incident at every stage of an attack, including: incursion, discovery, capture, and exfiltration.

51. At the first stage and second stages, incursion and discovery, data security measures are designed to prevent external users from entering into corporate networks and designed to limit users who enter into a corporate network for escalating their access and privileges, preventing unauthorized users from taking the necessary steps to identify and steal data. These measures include appropriate user training to prevent phishing attacks, maintaining strict control over user privileges so that users are not permitted to escalate their authority or enter unauthorized areas of the network, and to strictly monitor user activity for inappropriate or suspicious behavior. Additionally, corporate networks are segmented from the CDE to prevent easy access into the networks where payment card data is transferred.

52. In Wawa's Data Breach, external hackers gained accessed to every single one of Wawa's stores and gas stations, indicating the hackers had access to Wawa's central corporate networks and used that access to breach each stores' CDE. Wawa's security measures were thus incapable of preventing the hackers from accessing the network and identifying the undoubtedly numerous suspicious actions they took on Wawa's own networks and servers over several months.


53. At the third stage, capture, data security experts and common data security standards require merchants to put in place measures designed to prevent the installation of malicious software. Basic, nearly universal measures, including anti-virus and anti-malware

software are recommended on both corporate networks and on the POS systems that process payment cards. These types of software are used both to identify malicious software and to prevent their installation altogether. Likewise, file integrity monitoring software, universally acknowledged as a basic security requirement, identifies material and suspicious changes to system and network files and notifies appropriate personnel of the changes.

54. The millions of customers' payment card data stolen during Wawa's Data Breach occurred because of basic, well-known card-scraping malware used in practically every data breach since 2013. Not only did Wawa's anti-virus and anti-malware (if any) fail to prevent the installation of the card-scraping malware at any of its locations, it likewise failed to identify the malware, allowing the Data Breach to continue for months completely unnoticed. Whatever file integrity monitoring Wawa had in place wholly failed to discover the likely significant amount of suspicious activity ongoing at every one of Wawa's restaurants.

55. At the fourth stage, exfiltration, measures are recommended and available to prevent data from leaving protected systems and being sent to untrusted networks outside of the corporate systems. IP whitelisting, which allows only specific IP addresses to connect to trusted corporate networks and networks within the CDE, prevents hackers from sending data outside the network even when they manage to identify and collect customer sensitive data. Similarly, system information and event monitoring (SIEM) programs are designed to track systems activity to look for suspicious connections and attempts to transfer files to or from untrusted networks.

56. Here, Wawa's data security measures fell well short of reasonable. Over the course of nine months, the hackers collected customer payment card data. On January 27, 2020, even after being allegedly locked out of Wawa's systems for over a month, the hackers posted more than 30 million payment cards collected from Wawa's stores on Joker's Stash:




**Brand NEW Huge 30M+ pcs Nationwide
"BIGBADABOOM-III" BREACH at JOKER's STASH!**

Brand NEW Huge **30M+ pcs** Nationwide Breach
30.000.000+ Perfect Pure Fresh TR2+TR1 Dumps
40+ US States
31.000+ Different Bins
more than **1M pcs** of EU/ASIA/ARABS/EXOTIC bins (100+ Different Countries)

BIGBADABOOM-III-EU-part1 (BBB3 BREACH) **EU/ASIA/WORLD TR1+TR2/TR2, HIGH VALID 90-95%**, uploaded 2020-01-27
BIGBADABOOM-III-US-part1 (BBB3 BREACH) **USA by STATE/CITY/ZIP TR1+TR2/TR2, HIGH VALID 90-95%**, uploaded 2020-01-27
BIGBADABOOM-III-US-part2 (BBB3 BREACH) **USA by STATE/CITY/ZIP TR1+TR2/TR2, HIGH VALID 90-95%**, uploaded 2020-01-27
BIGBADABOOM-III-US-part3 (BBB3 BREACH) **USA by STATE/CITY/ZIP TR1+TR2/TR2, HIGH VALID 90-95%**, uploaded 2020-01-27

Be READY for the BIG-BADA-BOOM! Exclusively ONLY at JOKER's STASH!



**ALL STUFF WILL BE AVAILABLE AT
11:00 PM (evening update) New York City Time, Monday, January 27**

57. The Joker's Stash post proves the hackers successfully exfiltrated millions of Wawa's customer payment card data. While Wawa has not admitted that the cards posted to Joker's Stash came from its Data Breach, data security experts and financial institutions confirmed the payment cards published on Joker's Stash were each used at a Wawa and the geographic mapping showed the cards were from locations where Wawa operates.⁴²

58. Ultimately, Wawa enacted unreasonable data security measures that permitted hackers to easily enter its corporate network, CDE, and POS Systems. Then, because Wawa failed

⁴² Krebs, *supra* note 2.

to implement reasonable security monitoring measures, the breach continued unnoticed until an estimated 30 million payment cards were compromised. The exposure window of March 4, 2019 to December 12, 2019 shows hackers infiltrated, resided in, and exported data from Wawa's systems for months without notice.

59. The Wawa Data Breach and the resulting payment card theft was preventable had Wawa implemented reasonable, industry-recommended data security standards. However, it failed to do so.

***Wawa's Unreasonable Data Security Measures
Failed to Comply with Known Data Security Protocols***

60. Wawa should have been on high alert to the susceptibility of POS systems to data breaches. Security experts have consistently warned about the susceptibility of POS systems in restaurants.⁴³ One expert warned businesses that “you can’t neglect POS system security” noting that “[a]ny POS terminal with an IP address and a connection to a business’s network is as vulnerable to compromise as all the other pieces of equipment in that network.”⁴⁴ The same expert stated “[i]t’s not only okay to be obsessive about testing your POS systems for vulnerabilities and compromises...it’s essential.”⁴⁵

⁴³ Leebro POS, *5 Lessons To Learn From A Restaurant POS Security Breach*, Pointofsale.com (last visited, Feb. 28, 2017), <https://pointofsale.com/201506256716/Restaurant/Hospitality/5-Lessons-to-Learn-from-a-Restaurant-POS-Security-Breach.html>.

⁴⁴ *Id.*

⁴⁵ *Id.*

61. Datacap Systems, Inc. wrote in early 2016, “[y]our POS system is being targeted by hackers. This is a fact of 21st-century business.”⁴⁶ The same article notes Verizon reported “99 percent of the time, POS environments were hacked in only a few hours . . . [and] in 98 percent of cases, hackers exfiltrated data in just a couple of days.” The reason for the number and significance of data breaches was “[s]imply put, too many businesses . . . practicing less-than-stellar POS security.”⁴⁷

62. Specific measures and businesses practices can reduce the likelihood hackers can successfully intrude into businesses’ POS systems and limit the effect of any malicious software installed on any POS system or device. In fact, the Online Trust Alliance, a non-profit organization whose mission is to enhance online trust, user empowerment, and innovation, in its 2015 annual report, revealed that 90% of data breaches in 2014 were preventable.⁴⁸ Similarly, in 2017, the Online Trust Alliance found more than 93% of incidents in 2016 were preventable.⁴⁹ The OTA

⁴⁶ *Point of Sale Security: Retail Data Breaches At a Glance*, Datacap Systems, Inc. (May 12, 2016), <https://www.datacapsystems.com/blog/point-of-sale-security-retail-data-breaches-at-a-glance#>.

⁴⁷ *Id.*

⁴⁸ Press Release, *OTA Determines Over 90% of Data Breaches in 2014 Could Have Been Prevented*, Online Trust Alliance (Jan. 21, 2015), <https://www.otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented>.

⁴⁹ Bradley Barth, Report: Number of Cyber Incidents Doubled in 2017, Yet 93 Percent Could Easily Have Been Prevented, SC Media (Jan. 28, 2018), <https://www.scmagazine.com/home/security-news/privacy-compliance/report-number-of-cyber-incidents-doubled-in-2017-yet-93-percent-could-easily-have-been-prevented/>

emphasized that “[o]rganizations must make security a priority” and “those that fail will be held accountable.”⁵⁰

63. The vulnerabilities that may exist in POS systems are well-known and highly publicized. Almost five years ago, a Symantec report listed vulnerabilities in POS systems that must be resolved to prevent entry into POS systems and theft of consumer purchasing information.⁵¹ First, Symantec recommended “point to point encryption” implemented through secure card readers which encrypt credit card information in the POS system, preventing “RAM-scraping” malware which extracts card information through the POS memory while it processes the transaction. Second, Symantec highlighted the need to utilize updated software to avoid susceptibility in older operating systems being phased out, like Windows XP or Windows XP Embedded. Third, Symantec emphasized the need to implement POS systems capable of accepting EMV chips in payment cards, preventing the directly transmission of credit card information. These basic data security measures, known long before the Wawa data breach, are still important for preventing data breaches today.

64. Datacap Systems recommends similar preventative measures in what they call the “Tripod of POS Security.”⁵² The “tripod” includes (1) implementing POS systems supporting EMV chip-based payment cards; (2) end-to-end encryption, which encrypts payment card data as soon as payment cards are swiped; and, (3) tokenization, which replaces credit and debit card numbers with meaningless series of letters and numbers, rendering any information collected by hackers meaningless.

⁵⁰ Online Trust Alliance, *supra* note 48.

⁵¹ See Symantec, *supra* note 19, at 11-12.

⁵² See Datacap Systems, *supra* note 46.

65. The payment card industry (including card brands MasterCard, VISA, Discover, JCB, and American Express) has also heightened security measures in their Card (or sometimes, Merchant) Operating Regulations. Card Operating Regulations are binding on merchants and require merchants to: (1) protect cardholder data and prevent its unauthorized disclosure; (2) store data, even in encrypted form, no longer than necessary to process the transaction; (3) comply with all industry standards.

66. The PCI Security Standards Council, founded by American Express, Discover, JCB, MasterCard, and VISA, promulgates data security standards (again, referred to as “PCI DSS”) developed to “encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures.” PCI DSS applies “to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS comprises “a minimum set of requirements for protecting data.”

67. PCI DSS 3.2, the version of the standards in effect at the time of the Wawa Data Breach, sets forth twelve detailed and comprehensive requirements that must be followed to meet six data security goals:

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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security for all personnel

68. Among other things, the PCI DSS required Wawa to: properly secure payment card data; not store cardholder data beyond the time necessary to authorize a transaction; maintain up-to-date antivirus software and a proper firewall; restrict access to payment card data on a need-to-know basis; establish a process to identify and timely fix security vulnerabilities; assign unique identification numbers to each individual with access to its systems; and encrypt payment card data at the point of sale.

69. Compliance with PCI DSS is required but comprises only a portion of the minimum protective action a business must take. Security experts warn that “[w]hile PCI DSS provides a framework for improved payment processing, it is clear that it has been insufficient to ensure the

security of modern retail POS systems. To truly improve the security posture of POS devices, organizations must take a more dynamic approach.”⁵³ In fact, “every company that has been spectacularly hacked in the last three years has been PCI compliant.”⁵⁴ Target, Home Depot, Neiman Marcus, Michael’s, Sally Beauty Holdings, Inc., Supervalu, Albertson’s and many other businesses subjected to data breaches were recognized as PCI DSS compliant at the time of the compromise.⁵⁵

70. Federal and State governments have likewise sought to introduce security standards and recommendations to temper data breaches and resulting harm to consumers and financial institutions. The FTC has issued numerous guides for businesses highlighting the importance of reasonable data security practices. The FTC notes the need to factor security into all business decision-making.⁵⁶ Data security requires encrypting information stored on computer networks; holding on to information only as long as necessary; properly disposing of personal information that is no longer needed; limiting administrative access to business systems; using industry-tested and accepted security methods; monitoring activity on your network to uncover unapproved

⁵³ Wes Whitteker, *Point of Sale Systems and Security: Executive Summary*, SANS Institute (Oct. 2014), <https://www.sans.org/reading-room/whitepapers/analyst/point-sale-systems-security-executive-summary-35622>.

⁵⁴ Sean M. Kerner, *Eddie Bauer Reveals It Was the Victim of a POS Breach*, eWeek (Aug. 19, 2016), <http://www.eweek.com/security/eddie-bauer-reveals-it-was-the-victim-of-a-pos-breach.html>.

⁵⁵ Whitteker, *supra* note 53, at 1.

⁵⁶ Federal Trade Comm’n, *Start With Security A Guide For Business, Lessons Learned from FTC Cases* (June 2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

activity; verifying that privacy and security features work; testing for common vulnerabilities; and, updating and patching third-party software.⁵⁷

71. The FTC has also taken an active approach in issuing orders against businesses for failing to adequately and reasonably protect customer data. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. The FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data.⁵⁸ These orders further clarify the measures businesses must take to meet their data security obligations.

72. Several states have specifically enacted data breach statutes requiring merchants to use reasonable care to guard against unauthorized access to consumer information, such as California Civil Code §1798.81.5(b) and Wash. Rev. Code §19.255, or that otherwise impose data security obligations on merchants, such as the Minnesota Plastic Card Security Act, Minn. Stat. §325E.64. New Jersey, where Wawa is headquartered, and Florida, where Plaintiff is located, both also require companies to timely disclose a data breach. 73 Pa. Stat. § 2301, *et seq.*; Fla. Stat. § 501.171.

⁵⁷ See *id.*; Federal Trade Comm’n, *Protecting Personal Information, A Guide For Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

⁵⁸ See, e.g., *FTC v. Wyndham Worldwide Corp., et al.*, No. 13:-CV-01887-ES-JAD (D. N.J. December 11, 2015); *In the Matter of LabMD, Inc.*, 2016-2 Trade Cas. (CCH) ¶ 79708 (MSNET July 28, 2016); *In the Matter of Gmr Transcription Servs., Inc.*, 2015-1 Trade Cas. (CCH) ¶ 17070 (MSNET Aug. 14, 2014); *In the Matter of Genelink, Inc.*, 2015-1 Trade Cas. (CCH) ¶ 17034 (MSNET Jan. 7, 2014).

73. States have also adopted unfair and deceptive trade practices acts, which prohibit unfair trade practices, including the failure to employ reasonable security processes to protect payment card data. *See Fla. Stat. §§ 501.201, et seq.*

74. In this case, Wawa was at all times fully aware of its data protection obligations for all Wawa franchise and restaurant locations because of, among other reasons, its participation in payment card processing networks. Wawa also knew of the significant repercussions of a data breach because of the numerous daily transactions of tens of thousands of sets of payment card data. Wawa further knew that because they accepted payment cards at Wawa restaurant locations which processed sensitive financial information, customers and financial institutions, including Plaintiff and the Class, were entitled to and relied upon Wawa to keep sensitive information secure from hackers.

75. Despite understanding the consequences of a data breach and the measures it could take to avoid a data breach, Wawa failed to comply with PCI DSS requirements and implement basic data security measures necessary to prevent and quickly halt any data security incident.

76. The culmination of Wawa's failed security measures was the breach of its POS systems at its corporate-owned restaurants, franchise restaurants or both, allowing hackers to compromise all of its over 850 gas stations and convenience stores, resulting in the theft of information on over 30 million payment cards.

77. Wawa failed to reasonably protect cardholder information, putting consumer financial accounts in jeopardy and forcing financial institutions, like Plaintiff and the Class, to take remedial action for Wawa's inadequate preventative security measures.

78. Wawa had every opportunity to take preventive measures to avoid a breach of its POS systems. First, Wawa had more than adequate notice about the potential for hackers to

infiltrate POS systems and rob customers of their credit and debit card information. Second, Wawa appreciated the consequences of such a breach, having been warned by Visa that gas stations were being targeted by cybercriminals looking to steal payment card data, and having witnessed numerous other major retail stores and restaurants experience data breaches. Third, Wawa had access to information from data security experts, the FTC, and the payment card industry identifying steps necessary to protect POS systems. Fourth, Wawa had available established guidelines from PCI DSS that offered at least, minimal levels of protection. Despite the resources indicating the degree of risk of POS data breach and the potential steps to stymie a data breach, Wawa failed to take reasonable and sufficient action to avoid a breach of its POS systems, including failing to meet even minimal data security requirements. While Wawa saved money by deliberately truncating its data security investments, it knowingly put itself at risk of a breach and Plaintiff at risk of incurring expenses necessary to remediate and limit the damages caused by a breach.

79. Had Wawa remedied the deficiencies in its POS systems, followed PCI DSS guidelines, and adopted security measures recommended by experts in the field, Wawa may have prevented data breach into its POS systems and ultimately, the theft of millions of customers' purchasing information.

80. Because Wawa failed to take reasonable protective measures to prevent a data breach, Plaintiff and the Class will be required to bear the costs of preventing and repaying fraudulent transactions made with credit and debit card information obtained through Wawa's POS systems.

81. As a direct and proximate result of Wawa's Data Breach, Plaintiff and the Class have suffered damages and injuries, including expenses related to the following: (a) cancelling or

reissuing credit and debit cards affected by the Wawa Data Breach; (b) closing any deposit, transaction, checking, or other accounts affected by Wawa's data breach, including, but not limited to, stopping payments or blocking transactions with respect to the accounts; (c) opening or reopening any deposit, transaction, checking, or other accounts affected by Wawa's data breach; (d) refunding or crediting cardholders to cover the cost of any unauthorized transactions relating to Wawa's data breach; (e) responding to a higher volume of cardholder complaints, confusion, and concern; (f) increasing fraud monitoring efforts; and (g) investigating the impact of the breach on the financial institution and its members.

82. In this case, Wawa's data breach compromised an estimated 30 million payment cards. The Credit Union National Association ("CUNA") estimates the average cost to reissue payment cards is \$8.02.⁵⁹ Additionally, Gemini Advisory estimates that the "median price of US-issued records from this breach is currently \$17."⁶⁰ Thus, impacted financial institutions may have suffered as much as \$240.6 million to \$510 million in damages as a result of the data breach, excluding the likely significant amount of fraud.

83. Additionally, because the payment card information stolen from Wawa and offered on Joker's Stash for the purpose of being used for fraudulent purposes, the risk of harm to financial institutions is further increased.

84. The Wawa Data Breach, therefore, likely cost Plaintiff and the Class tens-of-millions of dollars in actual expenses for remediating and mitigating the damages it caused.

⁵⁹ *Visa tiers reimbursement costs for reissuing breached cards*, Credit Union Nat'l Assoc. (May 21, 2015), <https://news.cuna.org/articles/106029-visa-tiers-reimbursement-costs-for-reissuing-breached-cards>.

⁶⁰ Alforov & Thomas, *supra* note 4.

CLASS ALLEGATIONS

85. Plaintiff brings this action on behalf of itself and all other similarly situated Class members pursuant to Rule 23(a), (b)(2) and (b)(3) of the Federal Rules of Civil Procedure and seeks certification of the following Nationwide 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 at Wawa's stores and gas stations during the Wawa Data Breach.

86. Additionally, Plaintiffs bring this action on behalf of a proposed Florida Subclass of similarly situated members:

All banks, credit unions, financial institutions, and other entities headquartered or otherwise located in Florida that issued payment cards (including debit or credit cards) used by consumers to make purchases at Wawa's stores and gas stations during the Wawa Data Breach.

87. Excluded from the class is Defendant and its subsidiaries and affiliates; all employees of Defendant; all persons who make a timely election to be excluded from the class; government entities; and the judge to whom this case is assigned and his/her immediate family and court staff.

88. Plaintiff reserves the right to modify, expand or amend the above Class or Florida Subclass definitions or to seek certification of a class or subclasses defined differently than above before any court determines whether certification is appropriate following discovery.

89. **Numerosity.** Consistent with Rule 23(a)(1), the members of the classes are so numerous and geographically dispersed that joinder of all Class members is impracticable. Plaintiff believes that there are thousands of members of the Class and the sheer number of alerts notifying financial institutions of compromised card payment information indicates the Class is numerous; however, 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.

90. **Commonality and Predominance.** Consistent with Fed. R. Civ. P. 23(a)(2) and with 23(b)(3)'s commonality and predominance requirements, this action involves common questions of law and fact which predominate over any questions affecting individual Class members and members of the Subclass. These common questions include, without limitation:

- a. Whether Wawa knew or should have known of the susceptibility of its POS systems to a data breach;
- b. Whether Wawa's security measures were reasonable in light of the PCI DSS requirements, FTC data security recommendations, and common recommendations made by data security experts;
- c. Whether Wawa owed Plaintiff and the Class a duty to implement reasonable security measures;
- d. Whether Wawa's failure to adequately comply with PCI DSS standards and/or to institute protective measures beyond PCI DSS standards amounted to a breach of its duty to institute reasonable security measures;
- e. Whether Wawa's failure to implement reasonable data security measures caused the breach of its POS data systems to occur;
- f. Whether reasonable security measures known and recommended by the data community could have reasonably prevented the breach of Wawa's POS systems;
- g. Whether Wawa acted unfairly and deceptively by utilizing unreasonable data security measures and knowingly placing the risk of a data breach on Plaintiff and the Class;
- h. Whether Plaintiff and the Class were injured and suffered damages or other losses because of Wawa's failure to reasonably protect its POS data systems and corporate network; and,
- i. Whether Plaintiff and the Class are entitled to relief.

91. **Typicality.** Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiff is a typical member of the Classes. Plaintiff is a credit union which issued payment cards compromised by the infiltration and theft of card payment information from Wawa's POS system. Plaintiff's injuries are similar to other class members and Plaintiff seeks relief consistent with the relief of the Class.

92. **Adequacy.** Consistent with Fed. R. Civ. P. 23(a)(4), Plaintiff is an adequate representative of the Classes because Plaintiff is a member of the Class and is committed to pursuing this matter against Wawa to obtain relief for itself and for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff has also retained counsel competent and experienced in complex class action litigation of this type, having previously litigated data breach cases. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's and Subclass's interests.

93. **Superiority.** Consistent with Fed. R. Civ. P. 23(b)(3), class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy, Individual litigation by each Class and Subclass member would strain the court system because of the numerous members of the Class and Subclass. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court. A class action would also permit financial institutions to recover even if their damages are small as compared to the burden and expense of litigation, a quintessential purpose of the class action mechanism.

94. Injunctive and Declaratory Relief. Consistent with Fed. R. Civ. P. 23(b)(2), Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

CLAIMS

COUNT I

Negligence

(On behalf of the Nationwide Class)

95. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

96. Wawa owed an independent duty to Plaintiff and the members of the Class to take reasonable care in managing and protecting payment card information. This duty arises from multiple sources.

97. At common law, Wawa owed an independent duty to Plaintiff and the Class to implement reasonable data security measures because it was foreseeable that Wawa's data systems and the payment card data those systems processed would be targeted by hackers and that, should a breach occur, Plaintiff and the Class would be harmed. Wawa knew or should have known that if hackers had breached its data systems, they would extract payment card data and inflict injury upon Plaintiff and the Class. Furthermore, Wawa knew or should have known that if hackers accessed payment card data, Plaintiff and the Class would be responsible for remediating and mitigating the consequences of a breach by cancelling and reissuing payment cards to their members and reimbursing their members for fraud losses, thereby incurring costs and damages as a direct result of Wawa's breach. Therefore, the foreseeable consequence of Wawa's unsecured, unreasonable data security measures was a data breach that harmed Plaintiff and the Class.

98. Additionally, Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45, required Wawa to take reasonable measures to protect cardholder data. Section 5 prohibits unfair practices in or affecting commerce, which required and obligated Wawa to take reasonable measures to protect payment card data Wawa may possess, hold, or otherwise use. The FTC publications and data security breach orders described herein further form the basis of Wawa’s duty to adequately protect sensitive card payment information. By implementing unreasonable data security measures, Wawa acted in violation of § 5 of the FTCA. Moreover, state consumer protection statutes and deceptive and unfair trade practices statutes, incorporate and prohibit the unfair conduct prohibited under § 5 of the FTCA.

99. Wawa is obligated to perform its business operations in accordance with industry standards, including the PCI DSS, to which Wawa is bound. Industry standards are another source of duty and obligations requiring Wawa to exercise reasonable care with respect to Plaintiff and the Class by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and the Class.

100. Wawa breached its duty to Plaintiff and the Class. Specifically, Wawa implemented unreasonable data security measures, including failing to utilize adequate systems, procedures, and personnel necessary to prevent the disclosure and theft of the cardholder data of Plaintiff and the Class’s members. Wawa’s unreasonable actions include implementing data security measures that could not reasonably prevent an intrusion and were insufficient to quickly identify and resolve a data security stage during multiple stages of the Data Breach and over the course of nine months.

101. Wawa was fully capable of preventing the data breach. Wawa knew of data security measures required or recommended by the PCI DSS, FTC, and other data security experts which,

if implemented, would have prevented the data breach from occurring at all, or, even if its POS systems were compromised, would have limited the scope and length of the breach. Wawa failed to take reasonable measures to secure its system, leaving it vulnerable to a breach.

102. As a direct and proximate cause of Wawa's negligence, Plaintiff and the Class have suffered and will continue to suffer injury, including, but not limited to cancelling and reissuing payment cards, changing or closing accounts, notifying members 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. They also lost 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.

103. Because no statutes of other states are implicated, Pennsylvania common law applies to Plaintiff and the Class's negligence claim.

COUNT II
Negligence *Per Se*
(On behalf of the Nationwide Class)

104. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

105. Wawa's unreasonable data security measures violate Section 5 of the Federal Trade Commission Act ("FTCA"). Although the FTCA does not create a private right of action, it requires businesses to institute reasonable data security measures, which Wawa failed to do.

106. Section 5 of the FTCA, 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 by retailers, restaurants and other businesses like Wawa of failing to use reasonable measures to

protect cardholder data. The FTC publications and orders described above also form the basis of Wawa's duty.⁶¹

107. Wawa violated Section 5 of the FTCA by failing to use reasonable measures to protect cardholder data and by not complying with applicable industry standards, including PCI DSS. Wawa's conduct was particularly unreasonable given the nature and amount of payment card data it obtained and the foreseeable consequences of a data breach at a national restaurant, including specifically the immense damages that would result to consumers and financial institutions like Plaintiff and the Class.

108. Wawa's violation of Section 5 of the FTCA constitutes negligence per se.

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

110. Additionally, the harm that has occurred is the type of harm the FTCA (and similar state statutes) was intended to guard against. The FTC has pursued over fifty 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.

111. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have suffered and continue to suffer injury, including but not limited to cancelling and reissuing payment cards, changing or closing accounts, notifying members that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing

⁶¹ See *supra*, note 75 (listing orders).

fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their members. They also lost 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.

112. Because no statutes of other states are implicated, Pennsylvania common law applies to Plaintiff and the Class's negligence per se claim.

COUNT III
Violation of the Florida Deceptive and Unfair Trade Practices Act,
Fla. Stat. §§ 501.201, et seq.
(On behalf of the Florida Subclass)

113. Plaintiff, individually and on behalf of the Florida Class, repeats and realleges each and every allegation contained above as if fully alleged herein.

114. The Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. §§501.201, et seq., prohibits unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of trade or commerce. *See* Fla. Stat. §501.204(1). The FDUTPA expressly provides that consideration be given to interpretations by the FTC relating to Section 5 of the Federal Trade Commission Act. *See* Fla. Stat. §501.204(2); *see also* Fla. Stat. §§501.202(3), 501.203(3)(a)-(c).

115. Plaintiff and Florida Class members are "consumers" as defined by Fla. Stat. §501.203.

116. Plaintiff and the Florida Class have members located in Florida whose payment cards were impacted by the Data Breach. For these Florida-based cardholders, Plaintiff and the Florida Class reimbursed them for fraudulent transactions and/or reissued payment cards impacted by the Data Breach. Thus, Plaintiff and the Florida Class suffered an injury in Florida.

117. The conduct constituting Wawa's unfair acts and practices under this claim occurred primarily and substantially in Florida because Wawa's unlawful conduct: (a) foreseeably impacted financial institutions located in Florida, which is where members of the Florida Class incurred losses and suffered damages; (b) foreseeably impacted consumers residing in Florida whose Payment Card Data was compromised in the Data Breach; and (c) otherwise interfered with trade or commerce in Florida.

118. Wawa advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

119. Wawa engaged in unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of trade and commerce, in violation of Fla. Stat. §501.204(1), including:

- a. Unreasonably adopting and maintaining data security measures that were inadequate to protect Payment Card Data, which was a direct and proximate cause of the Wawa Data Breach;
- b. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following well-publicized cybersecurity incidents at other restaurants and retailers, which was a direct and proximate cause of the Wawa Data Breach;
- c. Failing to comply with the common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45, and Florida's data security statute, Fla. Stat. §501.171(2), which was a direct and proximate cause of the Wawa Data Breach;

- d. Misrepresenting that it would protect Payment Card Data, including by implementing and maintaining reasonable security measures; and
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of Payment Card Data, including duties imposed by the FTCA, 15 U.S.C. §45, and Florida's data security statute, Fla. Stat. §501.171(2).

120. Wawa's conduct is not only deceptive, but unfair and unconscionable within the meaning of FDUTPA because it constitutes immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Wawa cut corners and minimized costs, instead placing the burden on financial institutions, like Plaintiff, to protect Payment Card Data. Further, the injuries suffered by Plaintiff and the Florida Class are not outweighed by any countervailing benefits to consumers or competition. And, because Wawa is solely responsible for securing its networks and protecting Payment Card Data, there is no way Plaintiff and the Florida Class could have known about Wawa's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Wawa's legitimate business interests, other than its conduct responsible for the Data Breach.

121. Wawa's conduct is also unfair or unconscionable within the meaning of FDUTPA because it undermines public policy that businesses protect personal and financial information, as reflected in the FTCA, 15 U.S.C. §45, and Fla. Stat. §501.171(2).

122. Wawa's unlawful acts and practices complained of herein affect the consumer marketplace and the public interest, including the 30 million U.S. consumers, including numerous

Floridians, and thousands of U.S. financial institutions, including banks and credit unions headquartered in Florida, affected by the Wawa Data Breach.

123. As a direct and proximate result of Wawa's unconscionable, unfair, and deceptive acts and practices, Plaintiff and Florida Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring accounts for fraudulent activity; and an increased, imminent risk of fraud and identity theft.

124. Plaintiff and Florida Class members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. §501.21; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. §501.2105(1); and any other relief that is just and proper.

COUNT IV
Declaratory and Injunctive Relief
(On behalf of the Nationwide Class)

125. Plaintiff repeats and re-alleges the allegations contained in every preceding paragraph as if fully set forth herein.

126. 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.

127. An actual controversy has arisen in the wake of the data breach at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the payment card data of Plaintiff and the Class. Plaintiff alleges Wawa's actions (and inaction) in this respect were inadequate and unreasonable and, upon information and belief, remain

inadequate and unreasonable. Additionally, Plaintiff and the Classes continue to suffer injury as additional fraud and other illegal charges are being made on payment cards Plaintiff and the Class issued.

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

129. Wawa owes a legal duty to secure and the sensitive financial information to which it is entrusted— specifically including information pertaining to credit and debit cards used by persons who make purchases at Wawa restaurants – and to notify financial institutions of a data breach under the common law, Section 5 of the FTCA, Card Operating Regulations, PCI DSS standards, its commitments, and various state statutes;

130. Wawa continues to breach this legal duty by failing to employ reasonable measures to secure its customers’ personal and financial information; and

131. Wawa’s breach of its legal duty continues to cause Plaintiff harm.

132. The Court should also issue corresponding injunctive relief requiring Wawa to employ adequate security protocols consistent with industry standards to protect its customers’ personal and financial information.

133. If an injunction is not issued, Plaintiff will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach of Wawa’s data systems. If another breach of Wawa’s data systems 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 for out-of-pocket damages that are legally quantifiable and provable, do not

cover the full extent of injuries suffered by Plaintiff, which include monetary damages that are not legally quantifiable or provable, and reputational damage.

134. The hardship to Plaintiff and the Classes if an injunction does not issue exceeds the hardship to Wawa if an injunction is issued. Among other things, if Wawa suffers another massive data breach, Plaintiff and the members of the Classes will likely incur 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.

135. 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, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

136. Wherefore, Plaintiff, on behalf of itself and other members of the Class, requests that this Court award relief against Wawa as follows:

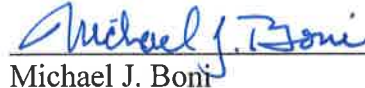
- a. An order certifying the class and designating Plaintiff as the Class Representative and its counsel as Class Counsel;
- b. Awarding Plaintiff and the proposed Class members damages with pre-judgment and post-judgment interest;
- c. Enter a declaratory judgment in favor of Plaintiff and the Class;
- d. Grant Plaintiff and the Class the injunctive relief;
- e. Award attorneys' fees and costs as allowed by law; and
- f. Award such other and further relief as the Court may deem necessary or appropriate.

JURY TRIAL DEMANDED

137. Plaintiff hereby demands a jury trial for all of the claims so triable.

Dated: February 19, 2020

Respectfully submitted,



Michael J. Boni
BONI, ZACK & SNYDER LLC
15 St. Asaphs Road
Bala Cynwyd, PA 19004
Telephone: (610) 822-0201
Facsimile: (610) 822-0206
mboni@bonizack.com

Brian C. Gudmundson
Michael J. Laird
ZIMMERMAN REED LLP
1100 IDS Center, 80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
michael.laird@zimmreed.com

Charles H. Van Horn
BERMAN FINK VAN HORN P.C.
3475 Piedmont Road, NE Suite 1100
Atlanta, GA 30305
Telephone: (404) 261-7711
Facsimile: (404) 233-1943
cvanhorn@bfvlaw.com

Jonathan L. Kudulis
KUDULIS REISINGER PRICE
17 North 20th Street, Suite 350
Birmingham, AL 35203
Telephone: (205) 251-3151
Facsimile: (205) 322-6444
jkudulis@trimmier.com

CIVIL COVER SHEET

20-cv-930

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
 INSIGHT CREDIT UNION

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

(c) Attorneys (Firm Name, Address, and Telephone Number)
 Michael J. Boni, Boni Zack & Snyder LLC
 15 St. Asaphs Road
 Bala Cynwyd, PA 19004; (610) 822-0201

DEFENDANTS
 WAWA, INC.

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)

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

Attorneys (If Known) _____

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

1 U.S. Government Plaintiff

2 U.S. Government Defendant

3 Federal Question (U.S. Government Not a Party)

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)

	PTF	DEF		PTF	DEF
Citizen of This State	<input type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input checked="" type="checkbox"/> 4
Citizen of Another State	<input type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business In Another State	<input checked="" type="checkbox"/> 5	<input type="checkbox"/> 5
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6

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

Click here for Nature of Suit Code Descriptions

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES	
<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	PERSONAL INJURY <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input checked="" type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input checked="" type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS Third Party 26 USC 7609	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 485 Telephone Consumer Protection Act <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS			
<input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	<input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer w/Disabilities - Employment <input type="checkbox"/> 446 Amer w/Disabilities - Other <input type="checkbox"/> 448 Education	Habeas Corpus: <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty Other: <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement			

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

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity)
 28 U.S.C. § 1332(d)

VI. CAUSE OF ACTION
 Brief description of cause
 Data breach caused by Wawa's negligent data security

VII. REQUESTED IN COMPLAINT: CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.C.P. DEMAND \$ 5,000,000.00 CHECK Y/N only demanded in complaint JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY (See instructions) JUDGE Hon. Gene E. K. Pratter DOCKET NUMBER 2:19-cv-06019 (E.D. Pa.)

DATE 2/19/20 SIGNATURE OF ATTORNEY OF RECORD Michael J. Boni FEB 19 2020

FOR OFFICE USE ONLY: RECEIPT # AMOUNT APPLYING IFP JUDGE MAG JUDGE

GEKP

UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF PENNSYLVANIA

20-cv-930

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: Insight Credit Union, 270 Winding Hollow Blvd., Winter Springs, FL 32708
Address of Defendant: Wawa, Inc., 260 W. Baltimore Pike, Wawa, PA 19063
Place of Accident, Incident or Transaction: Various

RELATED CASE, IF ANY:

Case Number: 2:19-cv-06019 Judge Hon. Gene E.K. Pratter Date Terminated

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

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

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

DATE 2/19/20 Michael J. Boni PA 52983
Attorney-at-Law / Pro Se Plaintiff Attorney I D # (if applicable)

CIVIL: (Place a check in one category only)

A. Federal Question Cases:

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

B. Diversity Jurisdiction Cases:

- 1 Insurance Contract and Other Contracts
2 Airplane Personal Injury
3 Assault, Defamation
4 Marine Personal Injury
5 Motor Vehicle Personal Injury
6 Other Personal Injury (Please specify)
7 Products Liability
8 Products Liability - Asbestos
9 All other Diversity Cases (Please specify) Class Action Fairness Act, 28 U.S.C. § 1332(d)

ARBITRATION CERTIFICATION

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

I, Michael J. Boni, 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 2/19/20 Michael J. Boni PA 52983
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

FEB 19 2020

GEKP

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

CASE MANAGEMENT TRACK DESIGNATION FORM

INSIGHT CREDIT UNION

on behalf of itself and all others similarly
situated,

v.

WAWA, INC.

⋮
⋮
⋮
⋮

CIVIL ACTION

NO. 20-cv-930

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. ()

2/19/20	<i>Michael J Boni</i>	Plaintiff
Date	Attorney-at-law	Attorney for
(610) 822-0201	(610) 822-0206	mboni@bonizack.com
Telephone	FAX Number	E-Mail Address

(Civ. 660) 10/02

FEB 19 2020