UNITED STATES DISTRICT COURT
DISTRICT OF DELAWARE

STEVEN SANDERS and PATRICIA SANDERS, on behalf of themselves and all others similarily situated, **PLAINTIFFS** **v.** **WAWA, INC.,** **DEFENDANT**	**CIVIL ACTION NO. _____** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiffs Steven Sanders and Patricia Sanders (collectively, "Plaintiffs"), individually and on behalf of all similarly situated Delaware persons and entities (collectively, the "Class" or "Class Members"), upon personal knowledge of the facts pertaining to themselves and on information and belief as to all other matters, complain of the wrongful actions of Defendant Wawa, Inc. ("Wawa"), and respectfully allege the following:

NATURE OF THE CASE

1. This is a data breach case. On December 19, 2019, Wawa revealed that it had discovered malicious software ("malware") on Wawa payment processing servers. According to Wawa, "[t]his 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" on December 12, 2019. Plaintiffs bring this class action on behalf of themselves and a Delaware Class against Wawa for failing to protect the personal and confidential information of millions of its customers—including credit card and debit card (also known as payment cards) numbers,

expiration dates, and cardholder names (collectively, "Payment Card Information"). Plaintiffs and Class Members have been injured and as a direct and proximate result of Wawa's wrongful disclosure of their Payment Card Information (the "Wawa Data Breach" or "Data Breach").

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 (CAFA), 28 U.S.C. § 1332(d)(2), as this is a class action in which the amount in controversy exceeds $5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists as Wawa is a citizen of a state different from that of at least one Class Member.

3. This Court has personal jurisdiction over Wawa because at all relevant times, Wawa regularly conducted (and continues to conduct) business in this District.

4. Venue is proper in this District, pursuant to 28 U.S.C. § 1391, because a substantial part of the wrongful conduct alleged herein occurred in, was directed to, and/or emanated from this District. Venue also is proper in this District because at all relevant times, Wawa regularly conducted (and continues to conduct) business in this District.

PARTIES

5. Plaintiff Steven Sanders is a citizen and resident of Newark, Delaware. Plaintiff Sanders paid for one or more purchases at a Wawa store and/or gas pump with a payment card between March 4, 2019 and December 12, 2019, and, on information and belief, his Payment Card Information was compromised in the Wawa Data Breach.

6. Plaintiff Patricia Sanders is a citizen and resident of Newark, Delaware. Plaintiff Sanders paid for one or more purchases at a Wawa store and/or gas pump with a payment card between March 4, 2019 and December 12, 2019, and, on information and belief, her Payment Card Information was compromised in the Wawa Data Breach.

7. Defendant Wawa, Inc. is a New Jersey corporation with its principal place of business in the Wawa area of Chester Heights, Pennsylvania in Greater Philadelphia. Defendant Wawa owns and operates over 850 convenience stores and gas stations in Delaware, Pennsylvania, New Jersey, Maryland, Virginia, Washington, D.C., and Florida.

FACTS

8. According to Wawa, "at different points in time after March 4, 2019, malware began running on in-store payment processing systems at potentially all Wawa locations." The malware "was present on most store systems by approximately April 22, 2019."

9. Wawa, however, did not discover the malware for over nine months after it infected Wawa's payment processing systems, and did not disclose the Data Breach for over a week after Wawa discovered it.

10. Although Wawa believes "this malware no longer poses a risk to customers using payment cards at Wawa," Plaintiffs and Class Members are subject to identity fraud and identity theft because of their compromised Payment Card Information wrongfully disclosed in the Wawa Data Breach.

11. Wawa had obligations, arising from promises made to its customers like Plaintiffs and other Class Members, and based on industry standards, to keep the Payment Card Information confidential and to protect it from unauthorized disclosures. Class Members provided their Payment Card Information to Wawa with the understanding that Wawa and any business partners to whom Wawa disclosed the Payment Card Information would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

12. Wawa claims it "is fully committed to data security." It further claims to "use security techniques on" its websites, "and through or in connection with our mobile apps or other

software- and Internet-enabled programs and services sponsored by Wawa (the "Sites") to help protect against the loss, misuse or alteration of information collected from [its customers] at the Sites."

13. According to Wawa, when customers "access [their] account information or transmit personally identifiable data to the Sites, that information is stored on servers that the Sites have attempted to secure from unauthorized access or intrusion. 'Secure Socket Layer' software encrypts personal information [its customers] transmit to the Sites."

14. However, Secure Socket Layer encryption protects information only during its transmission, but not when stored on Wawa's payment processing systems.

15. The Wawa Data Breach demonstrates that Wawa failed to honor its duties, representations, and obligations to protect Plaintiffs' and Class Members' Payment Card Information by, *inter alia*, failing to maintain an adequate data security system to protect against (and reduce the risk of) data breaches and cyberattacks, failing to adequately monitor its payment card processing systems to identify data breaches and cyberattacks, and failing to adequately protect Plaintiffs' and the Class Members' Payment Card Information.

16. Plaintiffs and Class Members have been injured and harmed by Wawa's wrongful disclosure of their Payment Card Information in the Data Breach.

17. Wawa's data security obligations and promises were particularly important given the substantial increase in data breaches leading to identity theft and identity fraud, which are widely known to the public and to anyone in the retail grocery and convenience store industries.

18. The United States Government Accountability Office ("GAO") noted in a June 2007 report on Data Breaches ("GAO Report") that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name." *Id.* at

2,9. Identity theft and identity fraud victims frequently are required to spend many hours and large amounts of money repairing the impact to their credit inflicted upon them by fraudsters using their purloined Payment Card Information.

19. There also may be a time lag between the time Payment Card Information is stolen and when it is used and once it is disclosed, fraudulent use of that information may continue for years;

> [L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft*. Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years*. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

GAO Report at 29 (emphasis added).

20. Payment Card Information, such as the Payment Card Information wrongfully disclosed in the Wawa Data Breach, is such a valuable commodity to identity thieves that once the information has been disclosed, criminals often trade the information on the "cyber black-market" for years—openly posting stolen Payment Card Information directly on various Internet websites and making the information publicly available. This fate could very well befall Plaintiffs' and Class Members' confidential Payment Card Information compromised in the Wawa Data Breach—and most likely already has.

21. Had Plaintiffs known that Wawa would not adequately protect their Payment Card Information and other sensitive information entrusted to it, they would not have made regular purchases at Wawa using their credit cards.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.