Wawa Data Breach Is Warning On Swipe Payment Tech Risks

By Adam Solomon and Anna Chan
Published in Law360 | September 19, 2022


A group of seven attorneys general recently announced an $8 million settlement with Wawa Inc. that resolves a multistate investigation into a significant payment card data breach at the company in 2019.

This settlement is one of the largest state attorney general settlements to date stemming from payment card breaches and serves as a reminder of the security and compliance risks associated with not fully migrating from swipe-based to chip-card transactions.

2019 Payment Card Breach

The Wawa payment card breach appears to have involved memory scraping malware that reportedly affected more than 850 store locations and fuel stations from April 2019 to December 2019, resulting in the compromise of approximately 34 million payment cards in total.[1]

The breach occurred after hackers gained access to Wawa's computer network allegedly through a phishing attempt targeting a company employee.[2]

The malware was capable of accessing and acquiring payment card information running on Wawa's payment processing servers, ultimately allowing the hackers to obtain magnetic stripe data and other cardholder data from cards swiped at Wawa's point-of-sale terminals.[3] Payment cards using chip technology were not compromised by the breach.[4]

In a press release published Jan. 28, 2020, Wawa informed the public of reports of criminal attempts to sell cardholder data purportedly related to the breach.[5] Wawa further stated that it had alerted its payment card processor, the payment card brands and card issuers to heighten fraud monitoring activities to protect customer information.[6]

The attorney generals alleged that Wawa failed to employ reasonable information security measures to prevent the data breach, violating the states' consumer protection and personal information protection laws.[7]

An investigation of the breach by a payment card industry forensic investigator found three violations of the Payment Card Industry Data Security Standard, or PCI DSS.[8]

Wawa Data Breach Is Warning On Swipe Payment Tech Risks
By Adam Solomon and Anna Chan
Published in Law360 | September 19, 2022

The Settlement

To resolve these claims, Wawa entered into an assurance of voluntary compliance with the participating attorney generals from New Jersey, Pennsylvania, Delaware, Maryland, Virginia, Florida and Washington, D.C.

Under the settlement, Wawa must improve its information security practices.[9] Wawa is required to create a comprehensive information security program that contains appropriate administrative, technical and physical safeguards, including implementing:

- Network segmentation of its cardholder data environment;
- Reasonable measures to detect and respond to security incidents within a reasonable time period;
- Reasonable access controls, e.g., multifactor authentication, one-time passcodes;
- Logging and monitoring controls; and
- Measures to ensure PCI DSS compliance.[10]

Wawa also must, among other requirements, undergo an information security compliance assessment by a third-party assessor within one year of the settlement.[11] The settlement also requires Wawa to pay $8 million in civil penalties, which is one of the higher fines issued by attorney generals in data breach actions in recent years.

Separate from the multistate attorney general settlement mentioned above, Wawa has also settled a consumer class action in April that resulted in the class members receiving approximately $9 million — in the form of cash and gift cards — and Wawa paying approximately $3.2 million to cover plaintiffs' legal fees and expenses.[12]

Advances in Payment Technology and PCI DSS

The settlement highlights the security and compliance risks associated with merchants that continue to use swipe payment technology at scale.

The push to migrate from swiping to chip technology or other secure payment methods has been ongoing, particularly with fueling stations and convenience stores.

In late 2019, Visa Inc. issued a security alert after investigating two separate breaches at North American fuel dispenser merchants, finding the

> threat actors were able to obtain payment card data due to the lack of secure acceptance technology (e.g., EMV, chip, point-to-point encryption, tokenization, etc.) and non-compliance with PCI DSS.[13]

Visa noted that

> the targeting of fuel dispenser merchants [was] the result of the slower migration to chip technology on many terminals, which made the merchants an attractive target for criminal threat actors attempting to compromise the POS systems for magnetic stripe payment data.[14]

Notably, Wawa upgraded the payment card readers at its fueling stations to chip technology in 2020.[15]

To incentivize the adoption of chip-enabled terminals by merchants, payment card brands offer exemptions to PCI compliance validation requirements to those merchants that, among meeting other requirements, process at least 75% of their annual transactions using chip technology.[16]

Importantly, these qualifying merchants still are required to comply with PCI DSS regardless of whether they are required to submit validation of their compliance to the card brands.[17]

In addition, the payment card brands have also shifted the liability associated with fraudulent point-of sale transactions from credit card issuers, such as bank or credit unions, to retail merchants who have not upgraded to chip technology.[18]

Recent updates to PCI DSS make it even more prudent for businesses to adopt appropriate payment technology for both in-store and online transactions. This past March, a new version of PCI DSS was released, marking the first major update in almost a decade since version 3.0 was issued.[19]

There are a number of new requirements in PCI DSS v.4.0, including stronger authentication, encryption, secure configuration and governance measures.

Despite the risk of hefty fines and other harmful consequences, full PCI DSS compliance among organizations remains low. The Verizon Wireless 2022 Payment Security Report found that around 43% of organizations globally maintained full PCI DSS compliance in 2020 based on data gathered by PCI DSS qualified security assessors.[20]

Although this number is underwhelming, it represents a notable improvement compared to 2019, where approximately 28% of organizations were estimated to maintain full PCI DSS compliance.[21]

Companies have a transition period up until March 31, 2024, to come into compliance with the new version of PCI DSS.

In preparation, businesses that come into contact with payment card information in any manner, should ensure their payment technology meets the industry standard and that a road map is in place to address the new PCI DSS requirements.

Wawa Data Breach Is Warning On Swipe Payment Tech Risks
By Adam Solomon and Anna Chan
Published in Law360 | September 19, 2022

Notes

1. Assurance of Voluntary Compliance (July 26, 2022), https://www.nj.gov/oag/newsreleases22/Wawa-Inc.pdf (last visited Sept. 12, 2022).

2. Press Release, New Jersey Acting Attorney General, Acting AG Platkin Co-Leads $8 Million Settlement with Wawa Inc. over Data Breach that Compromised Millions of Payment Cards In New Jersey (July 26, 2022), https://www.njoag.gov/acting-ag-platkin-co-leads-8-million-settlement-with-wawa-inc-over-data-breach-that-compromised-millions-of-payment-cards-in-new-jersey/ (last visited Sept. 11, 2022).

3. Id.

4. Id.

5. Assurance of Voluntary Compliance (July 26, 2022), https://www.attorneygeneral.gov/wp-content/uploads/2022/07/2022-07-26-PA-OAG-v.-Wawa-AVC-Accepted-efiling.pdf (last visited Sept. 14, 2022).

6. Id.

7. Id.

8. Id.

9. Assurance of Voluntary Compliance (July 26, 2022), https://www.nj.gov/oag/newsreleases22/Wawa-Inc.pdf (last visited Sept. 12, 2022).

10. Id.

11. Id.

12. In Re Wawa, Inc. Data Security Litigation, No. 2:19-cv-06019 (E.D. PA. April 20, 2022).

13. Visa Security Alert, "Attacks Targeting Point-Of-Sale at Fuel Dispenser Merchants" (November 2019), https://usa.visa.com/dam/VCOM/global/support-legal/documents/visa-security-alert-attacks-targeting-fuel-dispenser-merchant-pos.pdf (last visited Sept. 14, 2022).

14. Id.

15. Pat Ralph, "Wawa Improving Payment Security at Convenience Stores in Wake of Data Breach," Phillyvoice, (Jan. 9, 2020), https://www.phillyvoice.com/wawa-improve-security-data-breach-credit-card-chip-reader-gas-pumps/ (last visited Sept. 14, 2022).

16. MasterCard, "Security Rules and Procedures Merchant Edition" (Feb. 22, 2022), https://www.mastercard.us/content/dam/public/mastercardcom/na/global-site/documents/SPME-Manual.pdf (last visited Sept. 14, 2022).

17. Id.

18. Paula Fernandes, "Still Not Accepting EMV Chip Cards? Why You Need to Switch?," Business News Daily (June 29, 2022), https://www.businessnewsdaily.com/7859-emv-technology-small-businesses.html (last visited Sept. 14, 2022).

19. Press Release, Payment Card Industry Security Standards Council, "Securing the Future of Payments: PCI SCC Publishes PCI Data Security Standard 4.0" (March 31, 2022), https://www.pcisecuritystandards.org/about_us/press_releases/securing-the-future-of-payments-pci-ssc-publishes-pci-data-security-standard-v4-0/ (last visited Sept. 11, 2022).

20. Verizon News Center, "2022 Verizon Business Payment Security Report: Preparing to navigate PCI DSS v4.0," (Sept. 8, 2022), https://www.verizon.com/about/news/2022-verizon-business-payment-security-report (last visited (Sept. 11, 2022).

21. Id.

Adam Solomon *is a counsel in the firm's global privacy and cybersecurity practice in the firm's New York office. Adam assists clients in identifying, evaluating and managing global privacy and information security risks and compliance issues. He can be reached at +1 (212) 309-1327 or asolomon@HuntonAK.com.*

Anna Chan *is an associate in the firm's global privacy and cybersecurity practice in the firm's New York office. Anna assists clients in identifying, evaluating, and managing privacy and information security risks and advises clients on federal, state, and international privacy obligations. She can be reached at +1 (212) 309-1194 or achan@HuntonAK.com.*