DATA BREACH ALERT

Inside the Wawa Payment Data Breach

Rippleshot

WHAT HAPPENED

+850 Stores

Wawa has +850 stores that customers could have shopped at that may be impacted by this large-scale data breach.

9 Months

Debit and credit cards during a 9-month span from March 4-Dec. 12 could be impacted by the breach

2 Types of PII

The company discovered malware capable of exposing card numbers, expiration dates and cardholder names.

2 Days to Contain

The breach was discovered on Dec. 12 and the malware threat was contained two days later on Dec. 14.

WHAT YOU NEED TO KNOW

- Wawa is a convenience store chain operating in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida, and Washington, D.C.
- Debit card PINs, credit card security codes and driver's license information for verifying age-restricted purchases are not believed to be affected.
- Malware was installed on Wawa's payment processing servers and was used to exfiltrate customers' names, credit card numbers, and expiration dates.
- The convenience store chain spokesman said they are unaware of any unauthorized card use as a result of the breach.

Questions? Reach out to Customer Success Manager Jesse Sherwood at jesse@rippleshot.com

DATA BREACH ALERT

Inside the Wawa Payment Data Breach

Rippleshot

What You Can Do About the Breach

- ❑ Manually identify the list of cards that may have been compromised.
- ❑ Determine which cards to re-issue, which cards to write decision rules against, and which cards to monitor based on mitigation strategies.
- ❑ Continue monitoring the velocity of fraud from compromised cards to adjust strategies.
- ❑ Be on the lookout for additional news and development on this breach.
- ❑ Monitor potential fraud In real-time to get ahead of incidents before they spread.
- ❑ Track the fallout of the breach to identify potential Incidents from compromised data.

Questions? Reach out to Customer Success Manager Jesse Sherwood at jesse@rippleshot.com

DATA BREACH ALERT

Inside the Wawa Payment Data Breach

Rippleshot

What Rippleshot Sonar Users Can Do

On the Fraud Forecast Page*:

- ❑ Continue reissuing based on the recommendations made on the Fraud Forecast page.
- ❑ If you are concerned about additional risk due to the scope of the breach, consider reissuing cards with high orange scores to prevent additional fraud.

On the CPP Page:

- ❑ Search for compromised Wawa store locations using the “Search by Store Name” feature on the CPP List page.

On the Alerts Page:

- ❑ Your customer success manager should have reached out to you offering to produce a list of card tokens that visited a Wawa location during the exposure date range.
- ❑ If you are interested, that list can be uploaded to your Alerts page. Once uploaded, you will have a targeted list of cards potentially impacted by this breach to review and take action on.

*A Fraud Forecast Score™ assesses each card’s total exposure risk to determine the probability that it will become fraudulent in the next 90 days.