Data Breach Alert

Inside the Macy's Ecommerce Card Skimming Breach

What Happened

7 Days of Exposure

A breach on macys.com was discovered 7 days after it was believed to have occurred. Reports indicate a card-skimming script was injected onto the online payment portal on Oct. 7 and discovered on Oct. 15

5 Types of PII Exposed

It's believed that names, addresses, ZIP codes, email addresses, payment card numbers, card security codes, and expiration dates were breached. The impacted number of consumers is unknown.

What You Need to Know

- The attack has been linked to Magecart, a cyber criminal group known for injecting payment card skimmers into ecommerce websites. The payment data stolen was submitted by shoppers onto payment/checkout pages.
- Macy's reported that it received an alert about "a suspicious connection between macys.com and another website," which led to an immediate investigation.
- The hacker group reportedly injected computer code onto two pages at macys.com: The checkout page if credit card data was entered and an order was placed, and the wallet page of a shopper's account page.

How to Take Action

- ❑ This breach affected online transactions, and could have impacted customers from any bank or credit union.
- ❑ Look for cardholder transactions at MACYS.COM, MACYS eCommerce, MACYS Online, and other variant names between Oct. 7 and Oct.15 2019.
- ❑ 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.

Data Breach Alert

Inside the Macy's Ecommerce Card Skimming Breach

What Rippleshot Sonar Users Can Do

Any suspicious activity related to cards used at macys.com during the impacted period will be accounted for in Sonar's Fraud Forecast™ scores.

- Institutions that regularly reissue based on Fraud Forecast recommendations are already proactively protecting your cardholders.
- For cards in this specific breach, fraudsters may accelerate usage now that the news of the breach has broken. You should consider monitoring changes in Fraud Forecast scores and increasing the frequency of reissuing red cards.
- To understand how else Sonar can help you identify impacted cards below is a guide to using the CPP List page.

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.

CPP List guide to identifying potentially compromised cards that visited macys.com during the period reported by Macy's (October 7-15).

- ❏ From the CPP List page, click the "Search by Store Name" dropdown.
- ❏ Search for MACYS .COM (note the extra space after MACYS and before the .COM)
- ❏ Click on the MACYS .COM CPP to view the CPP detail: potentially impacted cards and where the related fraud occurred.
- ❏ Export these cards for monitoring or re-issuance.
- ❏ You can use the potentially affected card list to take action on a specific account.

When a network alert is issued, you can view the cards pinpointed for reissue in the Alerts section of Sonar.

Questions? Reach out to Jesse Sherwood,
Director of Customer Success: Jesse@rippleshot.com.

Rippleshot
Stopping Fraud at the Speed of Data