United States Secret Service Cybercrime Investigations

Cyber Security Alert
Evolving POS Skimming

The United States Secret Service is investigating a new payment card skimming device design used by criminals to target businesses with point-of-sale (POS) terminals.

Understanding the Threat

POS terminals are electronic devices designed to accept and process payments for business transactions, and include hardware and software, card swipers, barcode scanners, receipt printers. Skimming devices (skimmers) are electronic devices that are illegally attached to POS terminals, ATMs, fuel pumps to collect and record information when payment cards are used for transactions. This information is then used to steel funds from accounts associated with the compromised cards.

EBT Debit Cards and Skimming

The Secret Service and its law enforcement partners have observed an increase in nationwide POS and ATM skimming related activity over the past 18-24 months. This is due in part to the targeting of EBT debit cards that lack EMV chips. This problem is intensified further in states that allow cash withdrawals from EBT cards, such as California. Alerts have been issued by other law enforcement agencies and reporting has also increased by the private sector and media. For example, FICO, the credit scoring and data analytics company, published an article in February 2023[1] detailing the more than 700 percent growth in U.S. card skimming fraud from 2021 to present, based on data from their FICO Card Alert Service.

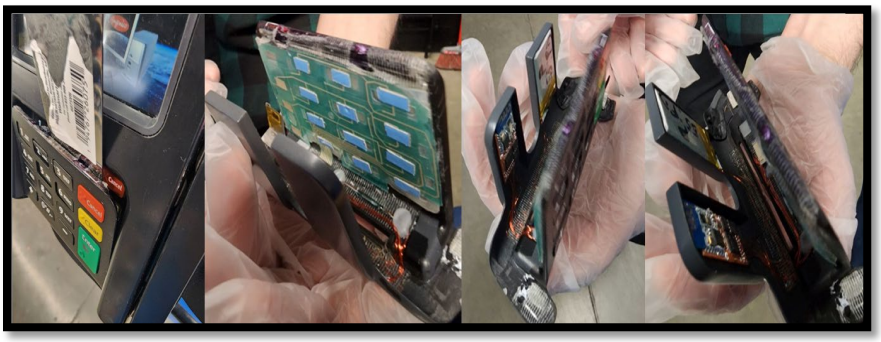
New Skimmer Design

The new skimmers, identified through investigations, only interfere with a small portion of the POS terminals, because they only capture data using the payment card's magnetic strip, not the EMV chip. However, they are designed to evade some of the basic methods of skimmer detection. They are made to either fit over the bottom half of the POS terminal or be concealed inside of the side of the terminal where cardholders swipe their magnetic strip cards. These devices are accompanied by a PIN pad overlay, which captures the cardholder's PIN entry. This type of POS skimmer is likely related to the ongoing targeting of EBT cards, which lack EMV chips, by organized crime groups.

[1] https://www.fico.com/blogs/us-card-skimming-grew-nearly-5x-2022-new-fico-data-shows

United States
Secret Service
Cybercrime
Investigations

Cyber Security Alert
Evolving POS Skimming



Cards that lack EMV chips present an easier target for organized crime groups to skim the card, re-encode the stolen magnetic strip data, and ultimately monetize the stolen card data through either unauthorized ATM withdrawals or fraudulent purchases.

Mitigation and Prevention for Businesses Using POS Terminals

Immediately take the POS terminal (or ATM) out of service to prevent further data compromise, make notification to your company's corporate security or loss prevention department, contact your local law enforcement agency, who can retrieve the skimming device and appropriately handle the device as evidence.

Mitigation and Prevention for Individual Cardholders

Immediately contact the card issuer's fraud department to report the incident, ask that the card be deactivated, and ask that a new card be issued with a new PIN. Monitor the affected account closely. If you suffered a financial loss as a result of the skimming incident, consider filing a fraud affidavit with the card issuer and contacting your local law enforcement agency to report the incident. In the future, consider making purchases using cards which can transact through contactless payment (i.e., tap-to-pay) or with the card's EMV chip, instead of the magnetic strip.