United States Secret Service Cybercrime Investigations

ALERT # 24-003-I

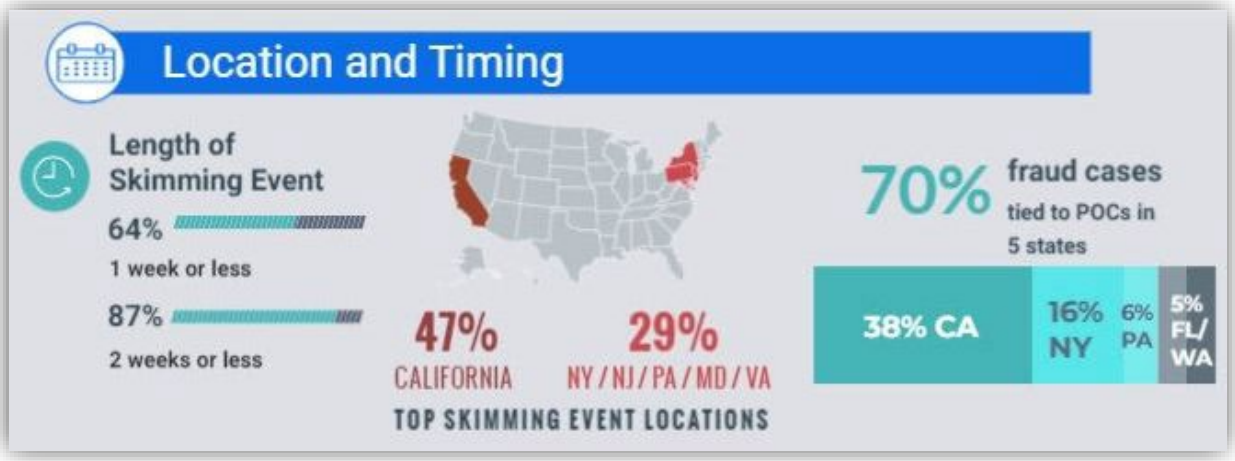
Criminal Investigative Division

Evolving Point-of-Sale Skimming Devices

The United States Secret Service is investigating a new skimming device design intended to target businesses with point-of-sale (POS) terminals. These new devices only interfere with a small portion of the POS terminals and are designed to be more difficult for businesses to detect, thereby resulting in fewer lost skimming devices and greater profit for organized crime networks.

Electronic Benefit Transfer (EBT) Debit Cards

The Secret Service Global Investigative Operations Center (GIOC) has 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. Intelligence 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.



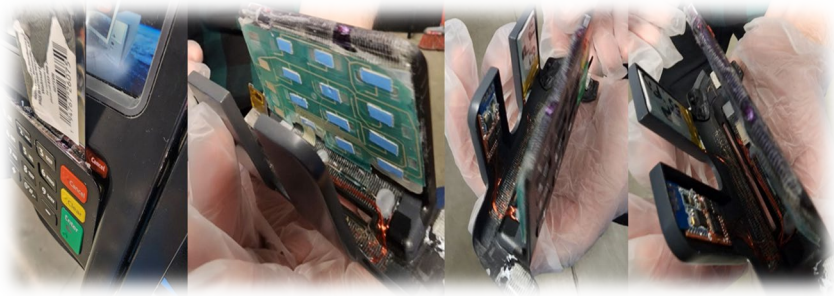
Source: https://www.fico.com/blogs/us-card-skimming-grew-nearly-5x-2022-new-fico-data-shows

These new POS skimming devices are designed to either fit over the bottom half of the POS terminal or be concealed inside of the side of the terminal where victim cardholders swipe their magnetic stripe cards. These devices are accompanied by a PIN pad overlay which captures the victim cardholder's PIN entry. These new devices make the more basic methods of skimmer detection less effective (i.e. pulling up on the four corners of the POS terminal).

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

Design

The below-pictured skimming devices are designed to capture only data from the cards magnetic stripe, not the EMV chip.



This is likely due to the ongoing targeting of EBT cards, which lack EMV chips, by organized crime groups. Cards that lack EMV chips present an easier target for organized crime groups to skim the card, re-encode the stolen magnetic stripe data, and ultimately monetize the stolen card data through either unauthorized ATM withdrawals or fraudulent purchases. According to information from law enforcement partners, most of the skimming device contraband intercepted while being imported to the U.S. is designed to target only magnetic stripe card data.

Mitigation and Prevention

Businesses

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 local law enforcement who can retrieve the skimming device and handle the device appropriately as evidence.

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(s) 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 police department to report the incident. In the future, consider making purchases using only credit cards which can transact through contactless payment (i.e. tap-to-pay or Apple Pay) or with the card's EMV chip. Paying with your card's contactless payment option or EMV chip is significantly more secure.

Contact your *local field office Cyber Fraud Task Force* to report.