UNITED STATES SECRET SERVICE

Public Advisory
ATM & POS Terminal Skimming

The United States Secret Service is the lead U.S. agency tasked with investigating access device fraud, a crime that affects consumers, businesses, and financial institutions. Skimming crimes account for hundreds of millions of dollars in losses annually to victims. Every year, the United States Secret Service responds to hundreds of ATM and skimming incidents by working closely with financial institutions and local law enforcement agencies.

How do Skimming Crimes Occur?

Skimming incidents involve criminal groups installing hidden electronic devices that record cardholder information at ATMs and Point-of-Sale (POS) terminals. These incidents occur frequently at popular merchants such as pharmacies, gas stations, and grocery stores. Criminals use the stolen (skimmed) debit or credit card data by re-encoding it on other cards for unauthorized ATM withdrawals or high-end purchases. Criminals may sell the stolen data from batches of cards to other groups.

ATM Skimming Devices

Criminals can insert ATM skimming devices deep inside an ATM's card reader slot, which are usually impossible to detect from the ATM's exterior. These devices can be designed to capture the data on the card's magnetic stripe or the card's Europay, Mastercard, and Visa (EMV) chip. ATM companies are constantly developing new security features to combat skimmers, but criminals adapt to these security features by changing their methods.

ATM Pinhole Cameras

Criminals can install hidden cameras on ATMs to record each cardholder entering their PIN. These cameras are often referred to as "pinhole cameras" because the lens can be as small as the tip of a ballpoint pen, which is easy to conceal on the ATM.

POS Skimming Devices

Criminals design plastic overlay shells that look identical to the top of the POS terminal and fit securely on the terminal. POS skimming devices cover the entire top exterior of the POS terminal, or just the keypad and EMV reader slot. Criminals use these skimming devices to capture the data on the card's magnetic stripe and the card's EMV chip. POS overlay skimming devices will also capture all keypad entries including the PINs. However, some merchants use high visibility security seals on the sides of POS terminals to make overlay skimming devices easier to detect.

Tips to Protect Yourself from Skimming

- Use ATMs that are inside of financial institutions, near security cameras, or close to the drive-up window. These ATMs are harder targets for criminals.
- Look for obvious signs of tampering at an ATM, such as broken lights, raised PIN pads with loose components, or stickers placed in unusual locations.
- Shield your PIN entry with another hand as much as possible to prevent a pinhole camera from recording your PIN.
- Inspect the exterior plastic edges of POS terminals and keypads for obvious signs of tampering. You can attempt to pull up on the corners of the terminal or the keypad's privacy cover. If any part of the terminal feels loose, do not use that terminal, and bring it to the attention of the merchant immediately.
- Consider using a credit card instead of a debit card to avoid potentially compromising your PIN and giving criminals access to your checking account.
- Sign up for any available text or email alerts that notify you when your card is used to help detect fraud.
- Consider making purchases using cards that can transact through contactless payments or with the card's EMV chip. Cards that lack EMV chips, such as Electronic Benefits Transfer (EBT) cards, are especially susceptible to targeting by criminal organizations. This is particularly true in U.S. states that allow cash withdrawals from EBT cards.

Continued on next page >

ATM & POS Terminal Skimming

What To Do If You Suspect Skimming

- **Businesses using ATMs or POS Terminals:** Take the ATM or POS terminal out of service immediately to prevent data compromise. Contact your company's corporate security or loss prevention department, or the company servicing the terminals. Contact your local law enforcement agency so they can retrieve the skimming device and handle it appropriately as evidence.
- **Individual Cardholders:** Contact your card issuer's fraud department immediately to report the incident, deactivate the card, and request a replacement card with a new PIN. Monitor any affected accounts closely. If you incurred financial loss, consider filing a fraud affidavit with the card issuer and contacting your local law enforcement agency.

ATM skimming devices

ATM pinhole camera

POS terminal skimming devices

How to Report Skimming Crimes

Report skimming incidents to your local law enforcement agency and/or the Internet Crime Complaint Center at https://www.ic3.gov. The United States Secret Service works closely with local and federal law enforcement agencies to investigate these crimes.