Five Tips to Fight ATM Skimming

ATM skimming is a global crime that incurs annual losses of $1 billion. At the basic level, thieves seek to extract cash from bank accounts; however, ATM skimming may just be the first step toward more intrusive identity theft as this type of crime becomes more organized and sophisticated.
According to the U.S. Secret Service, ATM skimming is becoming more common and increasingly organized. With technology always improving, well-funded criminal groups find it easier to steal money electronically than by personal confrontations. ATM skimming most often occurs after banking hours but during high-traffic times, such as weekdays from 5 to 10 p.m. and after 1 p.m. on weekends, in big, busy cities. The thieves hope to capitalize on unsuspecting citizens who are too busy to carefully inspect tampered ATM machines.

**High-Tech Theft**

Skimming devices can vary in sophistication. A standard skimmer is an electronic device that is placed on top of an ATM card reader. The device can be installed in under two minutes and seamlessly blends into the ATM’s facade, making it virtually undetectable. It’s important to note that even these basic skimmers are not generic off-the-shelf products. They have been carefully designed to target specific ATM models, matching the color and material of the ATM exactly. This tactic decreases the potential of being discovered.

Once an ATM card is inserted, the device includes a magnetic-strip reader that scans the card along with the ATM’s legitimate card reader. The skimmer’s reader captures and stores the banking data. With basic skimmers, the thief must return to remove the device in order to access the stolen data. Once retrieved, thieves download the data and re-encode it on another card with a magnetic strip. More advanced skimmers, however, do not require the device to be retrieved. Via Bluetooth or GSM technology, the device automatically sends the card data to a nearby laptop or cellphone or via text message.
Stealing the bank account information is only the first part. The thieves must also capture the ATM pin code. Pinhole cameras built into paneling that exactly matches the material and color of the ATM are positioned to capture and store video of customers entering pin codes. Hidden cameras can also be disguised as signs or bank literature holders on the ATM. Pin pad covers may also be employed to capture keystrokes; however, this is a riskier method because they are touched by the customers, who may sense the keypad doesn’t feel right.

Advanced skimmers involve all-in-one units — devices that include the skimmer and pinhole camera in one unit — and ultra-thin skimmers that are inserted inside the ATM card reader slot to scan and capture data from the magnetic strip.

Once in possession of a re-encoded bank card and the pin code, thieves are able to use the ATM to withdraw funds from the account.

Common Skimming Operations

The majority of ATM skimming attacks are committed by foreign criminal organizations. A typical ATM skimming hierarchy includes the top-echelon leadership, who are usually based in their homeland; a cell leader who secures devices from a device maker and directs a two-to-three-person install/recovery team; and a re-encoder.

Best Practices to Fight ATM Skimming

Banks can employ a number of best practices to prevent or minimize losses from ATM skimming.
1 Educate frontline employees about ATM skimming

Employees who are aware of this type of crime and understand the tactics play crucial roles in reducing ATM skimming. Banks should make it a priority to educate frontline employees, such as bank managers and tellers, about what ATM skimming is, how it works, the devices used, the most probable times it occurs, the duration of the incidents and the thieves’ modus operandi.

2 Conduct multiple daily inspections

Once bank employees are thoroughly trained, they should conduct multiple daily inspections of all ATMs, door access devices and teller pin pads, and their surroundings. At the minimum, these inspections should be conducted upon arrival, at midday and prior to closing. The more frequent the inspections, the better. Laminate photographs of how the ATMs should look so employees can compare the machines during inspections. Train them to look for seams and evidence of past skimming incidents, such as double-sided tape, glue residue and pry marks around the card reader. Report all damage and evidence to law enforcement and internal personnel. Review video footage to determine any suspects, view the time of install and removal, and identify potential affected cards so they can be blocked.
3 Use anti-skimming technology for ATM machines and door access devices

Banks can also purchase anti-skimming products and technology to prevent and minimize ATM skimming.

**These include:**

- Skimmer attachment prevention devices
- Card slot jiggle technology
- Frequency detectors
- Video variance detection
- Roving inspection patrols
- Anti-skim technology for door access devices
- Intelligent video surveillance platforms that feature real-time monitoring, alerting and investigative capabilities.

With platforms such as 3VR’s video intelligence solutions, banks can uncover and evaluate suspicious activity at ATMs in real time by correlating external data with 3VR Video Analytics and alerts. And when suspects are identified, 3VR’s platform integrates facial recognition analytics with alarm systems to search for known suspects and accomplices.

**If bank employees witness cases of active skimming, they should:**

- Immediately notify law enforcement
- Safely monitor the ATM until law enforcement arrives
- Do not confront the suspect(s) at any time
- Do not touch or remove the device
- Deactivate the ATM machine
- Identify the time of install and obtain footage of suspect(s)
- Block the reissue of cards
- Circulate internal alerts to warn other branches
4 Educate customers on safe banking practices and how to detect skimming equipment

Just as banks should educate employees, they should also educate their customers about skimming. Encourage them to inspect the machine prior to inserting the ATM card. They should even tug or jiggle the card reader and the keypad since most of skimming devices are adhered using double-sided tape. One of the most important and simplest ways to foil thieves is to cover the pin while it is being entered. Lastly, customers should immediately report suspicious incidents or damage to bank employees.

5 Use collaboration services

Collaboration services enable the sharing of vital evidence and best practices quickly between financial institutions, industry associations and law enforcement.

- 3VR’s CrimeDex is an online community comprised of more than 4,000 fraud, loss prevention and law enforcement professionals dedicated to stopping crime. Together, using 3VR’s Video Intelligence Platform, they can share, search and leverage relevant information on more than 15,000 suspected criminals between businesses and law enforcement.

- The ATM Skimming Intelligence Network is a global group of more than 400 law enforcement, banking security officials and ATM manufacturers. The group has assisted in identifying POCs and known ATM skimming suspects and provides intelligence to financial institutions and law enforcement.

Summary

By understanding ATM skimming, the technologies used, the modus operandi and the correct actions to take if incidences occur, and by employing anti-skimming products and services, banks can help their customers secure their assets and identity.
What is Video Intelligence?

3VR’s patented Video Intelligence Platform features real-time monitoring, alerting and investigative capabilities. With platforms such as 3VR’s, banks can uncover and evaluate suspicious activity at ATMs in real time by correlating external data with 3VR Video Analytics and alerts. And when suspects are identified, 3VR’s platform integrates facial recognition analytics with alarm systems to search for known suspects and accomplices.

Learn More

Contact 3VR at 877-387-6061 or info@3VR.com to learn more about 3VR’s Video Intelligence Platform or to request a demo.

Thanks to Detective Mark Solomon of the Greenwich Police Department for his insightful contributions to this paper.