Quick Reference Guide

prepared by:

CONEXXUS

NATIONAL ATM COUNCIL

Skimming Detection & Deterrence *for Convenience Store ATM Owners*

What is ATM Skimming?

Skimming is the theft of credit/debit card information by a device placed in, on, or around an ATM. These devices allow criminals to secretly record credit/debit card information (from the magnetic stripe) - for later use in fraudulently producing counterfeit cards. ATM skimming also includes capturing customer PINs associated with the cards using a hidden micro camera that records the PIN digits, Keypad overlays, and "shoulder surfing", are other methods.

What is the Skimming Threat for My Store ATMs?

Although convenience stores and other indoor retail ATMs have traditionally not been targeted by criminals, skimming now appears to be on the rise as criminals sense a "closing window of opportunity" with the new and more secure EMV chip cards and EMV updated terminals now being implemented in the U.S.

It's very important to know how to detect and deter skimming at your store ATMs in order to continue providing a safe environment for your customers. This Guide outlines steps you can take to help stop skimming and what to do if/when your ATM is ever compromised by a skimming device.

What Can I Do To Maintain and Maximize a Safe Environment for My Store ATMs?

There are several steps you can take to help reduce the threat of skimming at your store(s):

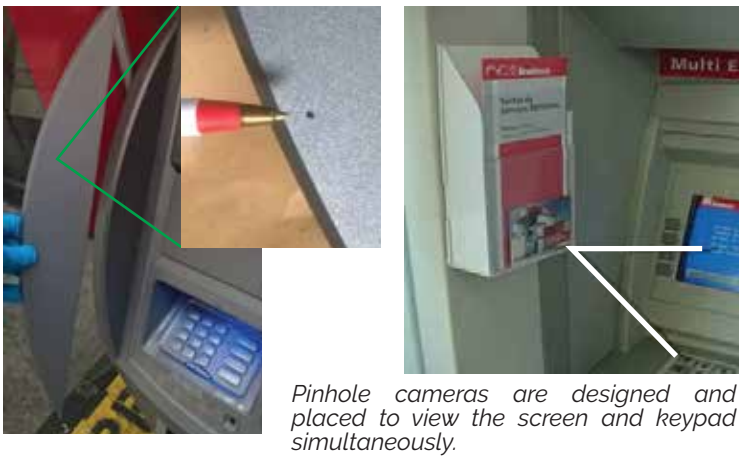
- **Place your ATM where it can be seen by your cashier AND make sure your video surveillance covers the ATM**
  Place an ATM in store locations where it: (i) will not be needlessly exposed to "smash & grabs"; (ii) is under line-of-sight visual surveillance by store personnel; and (iii) does not expose communications cables or other points of entry/exit to the ATM's components or communications. Be sure your video surveillance captures the face of the person using the ATM and not PIN entry or display screen information.
- **Train your employees**
  Use this Guide as a key part of training employees. Keep a copy at the cash register for easy reference, but be careful to keep it secure, out of sight, and accounted for at all times.
- **Know your ATM**
  You and your employees should familiarize yourselves with exactly what the ATM(s) in your store(s) look like without any skimming devices installed. Take photos of the ATM so you have a comparison for reference. Remember, criminals are very good at making skimmers look like they "belong" – so a good mental and physical image of your unaltered ATM is important when making the regular inspections needed to detect skimming.
- **Inspect your ATM on each shift or at least once a day**
  Each shift manager should perform an ATM inspection. This takes only a short time, but is perhaps the most important element in a comprehensive anti-skimming program.
  > There are two basic categories of skimming devices: internal and external. External skimmers are placed on the outside of the card slot – on top of the ATM card reader. Internal skimmers are placed inside the card slot and are more difficult to detect. You should be checking for both types of skimmers.

Internal ATM Card Slot Skimmer

> **Examine your ATM card reader.**
  Check the card reader opening by jiggling/pulling on the card reader itself. It should be solid and not move. Most skimmers are temporarily installed with double-sided tape and will come off easily if pulled. Look inside the card slot to see if any device has been placed within the normal space, or if anything looks "different" in the size or shape of the card slot. Push a non-functioning card, such as a non-activated gift card, into the slot to test whether the card goes in smoothly, or feels "different" – indicating an internal skimmer has been installed.

External ATM card reader overlay skimmers are designed to look very similar to the machine's card reader - but have minor differences that are recognizable if you know your machine.

> **Look for a micro camera.**
Cameras used by criminals are tiny and usually hidden in items such as a literature holder or disguised as a component of the ATM enclosure itself with line of sight to the keypad.



Pinhole cameras are designed and placed to view the screen and keypad simultaneously.

PIN Pad Overlay

> **Inspect for a keypad overlay.**
These go right on top of the ATM key pad and are normally secured with double-sided tape. Again, jiggle and "pressure test" the key pad. Look for a lip around it that wasn't there before. Look closely and notice whether the color, texture, etc. are different.

> **Inspect for internal skimming device.**
If you have authorization/access to the interior of your ATM, check for an internal skimming device. Internal devices include those placed inside the ATM cabinet and connected directly to the card reader or to the computer board that controls the card reader/captures the card data. These and other skimming devices may have Bluetooth wireless capability to transmit stolen card data to criminals. Request that your ATM service provider/vendor show you exactly what to look for -- and then incorporate an internal examination into your regular ATM anti-skimming regime.

> **Use Bluetooth/Wi-Fi Scanners.**
Use one of the free Bluetooth/Wi-Fi scanner apps available for most smart phones to regularly scan for any new/unrecognized signals/devices. Run a "baseline" scan of your store, making note of the "normal" signals/networks/devices, so you can detect any changes in subsequent scans.

What Other Protective Steps Should I Take?

Check with your ATM vendor about available anti-skimming devices for your ATM(s) – to thwart ever more sophisticated skimming techniques and devices from the criminals. These devices range from physical attachments constricting card slot entry to newer card readers with embedded anti-skimming electronics that detect/alert you to placement of a skimmer, and may emit "jamming signals" and encrypt card data.

What Should I Do Right Now?

As an important first step, contact local law enforcement now, before a skimming incident occurs, and ask for advice on their preferred course of action in the event you do find a skimming device on your ATM. Write down the instructions and let your ATM vendor/service provider know of this local protocol for their feedback and confirmation. Follow the steps outlined by local law enforcement wherever possible.

What Should I Do To Educate My Customers?

Use the ATM screen display and physical signage to remind your customers to always cover the key pad and their finger movements with the other hand when entering their PIN. This simple step is key to keeping customers' most sensitive information safe.

What Should I Do If I Find a Skimming Device In/On My Store ATM?

1. Be careful not to touch the skimming device itself, but immediately place an "Out of Order" sign on the ATM. Follow the protocol provided to you by local law enforcement - including contacting them immediately to advise of a skimming device found on your ATM. Ask them to come to your store so they can obtain evidence and you can file a report. (You may also wish to contact your closest regional US Secret Service office.)
2. Contact your ATM vendor immediately and let them know you believe you have found a skimming device on your ATM. Let them know you have also contacted law enforcement and ask your ATM vendor to coordinate with them to ensure the safe/secure removal of the skimmer and restoration of the ATM to normal service. If you "self-service" the ATM, and local law enforcement does not arrive promptly (within 2-3 hours where the ATM is critical to your business), follow these steps before restoring the ATM to service:
   > Take photos of the skimming device as installed.
   > Remove the device with as little handling/destruction as possible, using protective gloves if available.
   > Store the skimmer/camera in a plastic bag to provide to law enforcement whenever they arrive.
3. Be alert to notice if there is a car/truck parked nearby for long periods of time. Bluetooth wireless can be used to retrieve card data from nearby skimming devices in real time. If you see someone suspicious, make a good mental note and discretely record the license plate/make/model/color/departing direction of travel and provide that information to the authorities.
4. If you observe a person attempting to recover the skimming device, DO NOT INTERVENE. Discretely note and write down the physical features of the person(s), their clothes, car/truck license plate number/make/model/color and direction of travel, and provide to law enforcement ASAP once the suspect leaves.

Version 01 / Effective 08/19/2016