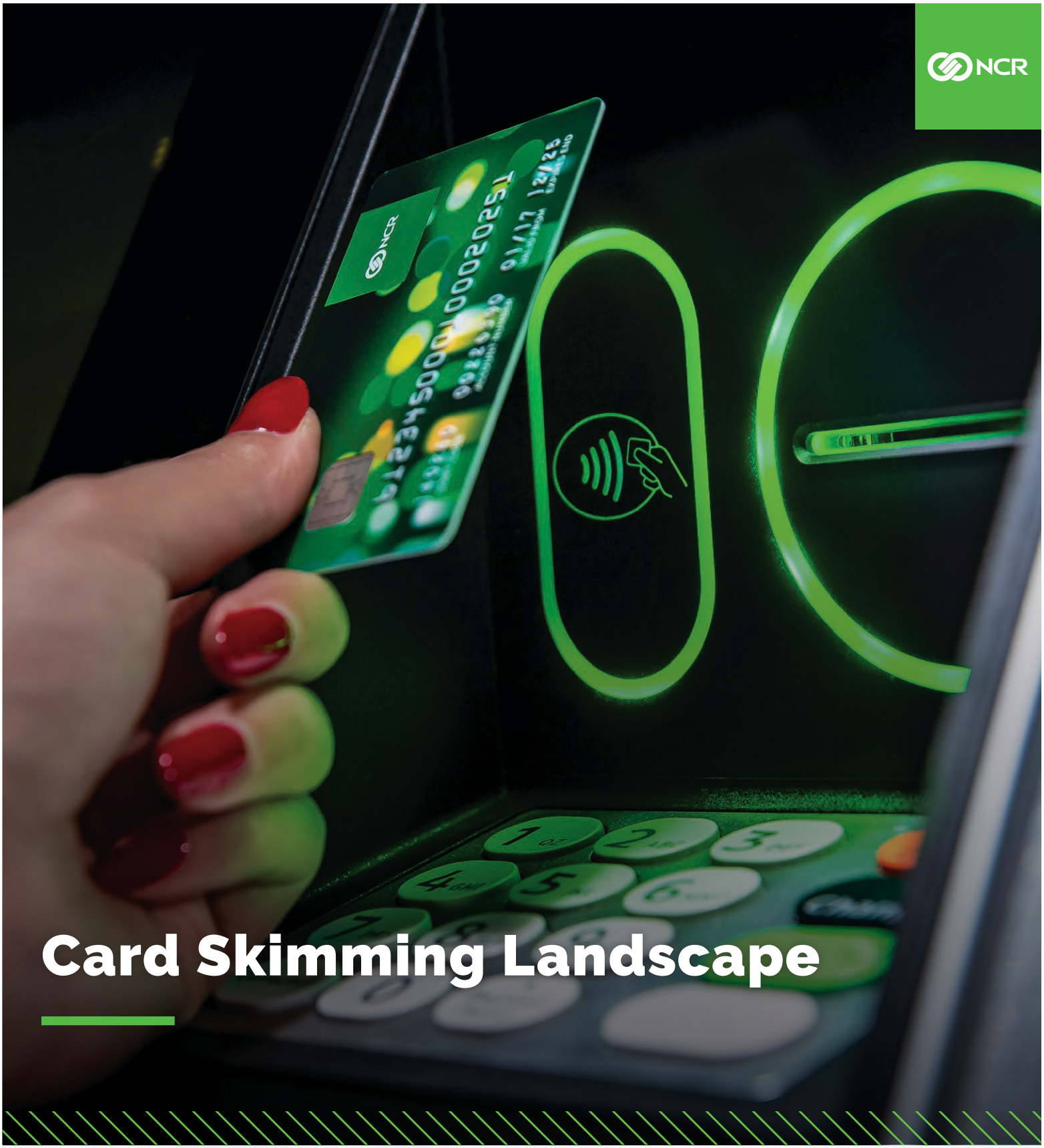


Card Skimming Landscape

Methods of Card Skimming at an ATM, and how to defend against them

An NCR white paper

October 2019

Card Skimming Overview

Card Skimming remains the biggest form of loss in the ATM channel, and while defences have been developed to prevent some forms of skimming, criminals have similarly worked to develop new skimming techniques to enable the crime to continue.

This has resulted in an arms race between the attackers and the defenders which is showing no signs of stopping. This paper will describe the current landscape with respect to card skimming, and also describe the defences available to protect an ATM. The final section of the paper will describe how the arms race can be avoided and end the opportunity for skimming completely.

What is card skimming?

Card skimming is defined as the process of unauthorized copying of magnetic strip data for the purpose of creating a cloned card. The PIN corresponding with this magnetic strip data is also required, and this is typically obtained at an ATM by observation of PIN entry during a legitimate transaction. Card skimming originally would occur by copying the data from a card as it was entered into the ATM, through the fitting of an additional card reading device to the ATM fascia. Today, card skimming can occur at any point within the ATM in which there is magnetic card data present.

2. Card Skimming Methods

Fascia skimming

Fascia skimming was the original form of skimming, and still represents a significant threat today. This is the 'traditional' way to skim a card, by adding a secondary, disguised reader to the ATM fascia. These devices are typically overlay devices or insert devices.

Internal Skimming

Deep Insert Skimming is a newer, but increasingly common, form of attack because it can avoid traditional fascia skimming defences. Internal skimming places the skimmer inside the card reader, often using the card slot as the method of entry/exit for the skimmer. These are commonly known as Deep Insert Skimmers, or M3 / D3 skimmers.

Eavesdropping

Card data can also be obtained by unauthorised connection with the card reader electronic components. Eavesdropping skimmers can get card data by connection with the read head, the pre-read head or the card reader control board. Eavesdrop skimmers are typically fitted by drilling a hole in the ATM fascia to gain access, and then disguising the hole.

USB Skimming

Card data is sent from the card reader to the ATM PC core over USB. A USB sniffing device connected inline with the USB cable can record card data. A USB skimmer would typically require access inside the ATM top box for fitting.

Software Skimming

Card data is vulnerable to capture within the ATM Software stack using skimming malware.

Communications Skimming

Card data is present on the communications channel between the ATM and the ATM Terminal handler. Typical locations for Communication skimmers are as inline sniffers connected to the network cable, sometimes within the ATM top box, sometimes outside the ATM cabinet.

Shimming

This is the technique of intercepting data from an EMV chip (on the top of the card). EMV chips contain track 2 equivalent data which is similar, but not exactly the same, as that found on the magnetic strip. All magnetic strip transactions must be accompanied by a valid magnetic CVV. If magnetic CVV is not validated as part of transaction authorization, then EMV cards could be vulnerable to card shimming.

2. Card Skimming Defenses

Fascia skimming

SPS — SPS will prevent fascia skimming by detecting skimmers on the fascia, and also by the electromagnetic jamming of skimmers (jamming for motorised card readers only). It can also be configured to take the ATM out of service if a skimmer is detected, or send an alert to an ATM monitoring system. SPS is also equipped with anti tamper sensors to prevent sabotage of the defence. Note: As with any detect function, SPS may experience false positives and this should be taken into account when implementing alert management policies

Internal Skimming

Tamper Resistant Card Reader — the TRCR has a narrowed card guide along the path of the track 2 data. This removes space required for a card to move correctly if a deep insert skimmer is fitted. On a Dip Card Reader the height of the card path is significantly reduced to make it almost impossible to fit both a skimmer AND a card.

Eavesdropping

Tamper Resistant Card Reader — the TRCR also has epoxy resin coating all electrical nodes which carry card data. This forms an insulating barrier that stops an eavesdropper from making a connection.

USB Skimming

Encrypted USB Communications in APTRA XFS 6.06 encrypts the card data by default over the USB link inside the ATM.a connection.

Software Skimming

NCR Hard Disk Encryption, BIOS locked and configured to boot only from primary hard disk **Hardened Operating System, Solidcore Suite for APTRA.** This solution combination is required to prevent the installation of malware whether using online or offline methods.

Communications Skimming

TLS1.2 encrypts the communications from the ATM to the transaction terminal handler. Ensure that TLS 1.2 is used over the complete link, and that there are no unprotected segments e.g. from ATM to router.

Shimming

Correct issuer authorization of magnetic strip transactions. The equivalent track 2 data will not have the correct CVV for a magnetic strip transaction, so issuer authorization systems can easily detect and deny any fraudulent transactions.

3. How to avoid the arms race

Card skimming remains a problem on the ATM because it is too easy for a criminal to capture and re-use the static information found on magnetic strip cards. The problem can be solved by the elimination of use of magnetic strips, and there are existing techniques which can be used to effectively discontinue the use of magnetic strip without the need to issue new cards.

Contactless EMV

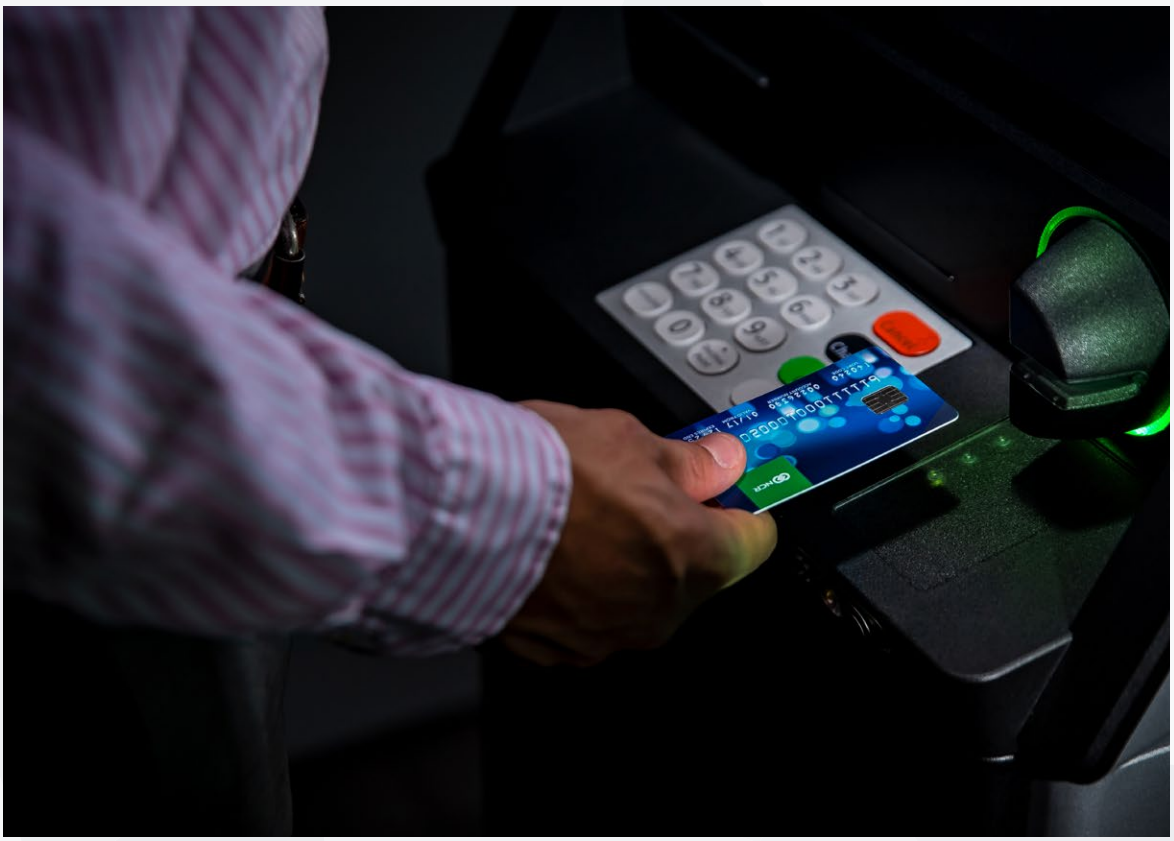
Replace card and PIN with Tap and PIN. Contactless EMV uses unique cryptograms in each transaction which cannot be reused if captured. The elimination of card insertion eliminates the opportunity for both fascia and internal skimming.

Geo-Blocking

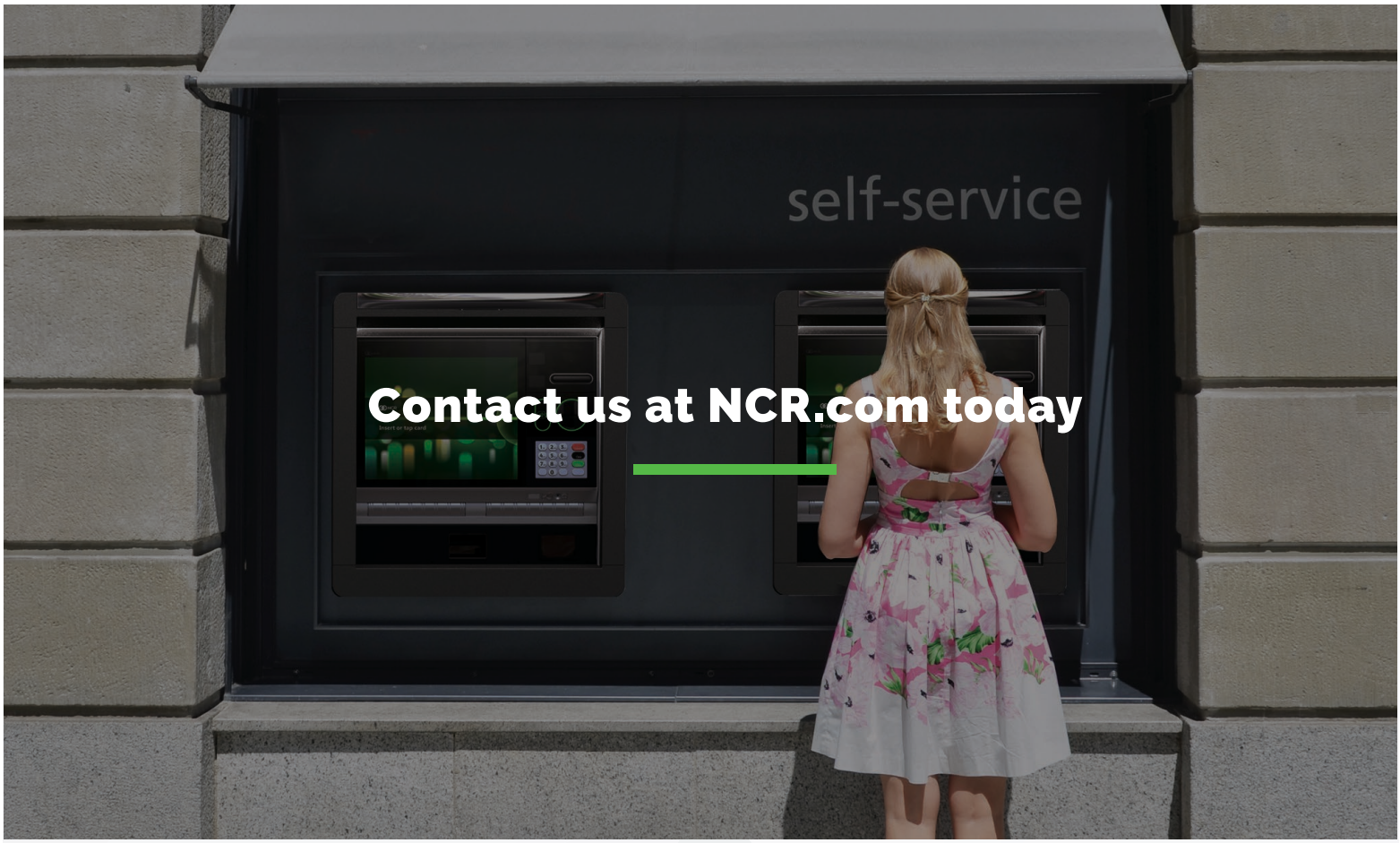
Issuers can block the authorization of magnetic strip transactions from non-EMV geographies. This prevents skimmed magnetic data from being used to create a valid cloned card.

Use Chip Only card reader

A chip only card reader only allows a card to be inserted far enough to read the chip, but not far enough to allow the magnetic strip to be skimmed.



Card Skimming Landscape



Contact us at NCR.com today

Why NCR?

NCR Corporation (NYSE: NCR) is a leading software and services-led enterprise provider in the financial, retail, hospitality, small business and telecom and technology industries. We run key aspects of our clients' business so they can focus on what they do best. NCR is headquartered in Atlanta, Ga., with 34,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries.