NCR TAMPER RESISTANT CARD READER

June 2019 – Update for Dip
Christine Bunch, Physical Security & Card Reader
Agenda

- Card Skimming Attack Trends
  - Business Impact
  - Deep Insert Skimming Overview
  - Eavesdropping Overview

- NCR’s Tamper Resistant Card Reader
  - Overview
  - Detail of Changes *updated for Dip*
  - Availability Dates

- ATM Advanced Card Protection Offer Details *new*

- Further Talking Points
The Business Impact from Card Skimming Attacks on ATMs

The most frequent form of attack on ATMs

- Card Skimming represents most of the total reported losses from ATMs
- Each Card Skimming Attack can cost over $50,000
- Card Data theft from ATMs is a key driver in overall card fraud
Card Crime Trends

Emergence of Deep Insert Skimming

Evolution of Eavesdropping Attacks
Deep Insert Skimming Overview

- Sits further into the card reader than typical insert skimmers
- Intent of this technique is to defeat jamming technology which focuses on the bezel
- Different styles of device observed
- Devices sometimes transmit card data in real time, sometimes on board storage
Deep Insert Skimmers - Variations

- Deep Insert Skimming often causes card jams
- Criminal has to physically open card reader shutter to retrieve the device and damages card reader in process
Eavesdropping Attacks Overview

- Break-through Fascia
- Attach to read-heads or control electronics within card reader module
- Fascia break-through “naturally” hidden
- Impact as per “traditional” skimming
Eavesdropping Skimming - Variations

Criminals cut a hole in the facia to attach a skimming device directly onto the card reader.

They then secure a pre-cut cover over the hole with double faced tape, it is easily missed with a simple glance.

With a close inspection you can see a seam on the facia where the overlay panel is installed.
Eavesdropping – Internal View

Card reader - Side view

Viewed from below
To combat emerging skimming techniques of Deep insert Skimming and Eavesdropping, NCR has hardened the card reader

- Small mechanical changes to the reader will have a great effect in improving security
- No electronic, firmware or software changes have been made, therefore no certification is necessary
  - In order to properly track introduction of the improved reader into customer estates, NCR has changed the part number and the feature number.
- No change to EMV approval numbers

NCR’s New Tamper Resistant Card Reader
New default card reader
## Tamper Resistant Card Reader Overview

### Key Features
- Reduced bezel gap and guideblock gap inside card reader
- An epoxy resin on various part of the PCB to protect the signals emitting from it
- Communication signals and data security
  - In addition to the hardware improvements, a separate XFS component is available to improve the security of the Communication signals and data from the card readers, in the form of encrypted USB comms
    - Released with APTRA XFS 06.06.00

### Key Benefits
- No need for additional 3rd party products to be included for added security (such as anti-skimming plates) – NCR is hardening the card reader against these forms of crime as default.
- Quicker and easier servicing – all components included within the card reader itself so no need to remove additional hardware to reinstall on replacement readers
- Drop in replacement for current card reader models – no additional firmware/ software or electronics required therefore no certification is necessary
- No change to EMV approval numbers
➢ To counteract ‘internal skimming’ device, gap **reduced** between upper & lower guideblock from 2.4mm to 1.35 (Δ 1.05mm) - internal to Card Reader

➢ To counteract ‘internal skimming’ at magnetic read-head, bezel gap is also **reduced** from 1.195 to 0.995mm (Δ 0.2mm)
Tamper Resistant Motorised Card Reader – change detail contd

Below shows the physical comparison for the bottom transport guide card reader models

New Guideblock design – inc. (i) raised moulding closes gap to 1.35mm (ii) closed area around Read Head

Current Guideblock design
Tamper Resistant Motorised Card Reader – Anti Eavesdropping Solution

Track-2 data is protected at various PCB sites by application of epoxy glue during production.
Tamper Resistant Dip Card Reader – Detail of changes

Includes Anti-eavesdropping protection

Gap reduced between upper & lower guide-block - internal to Card Reader from 1.3mm to 0.84mm
Tamper Resistant Card Reader Availability

**Key Dates – Motorized**

- **Features (F505, F507)**
  - Orderable since Oct 2017
  - Default since Jan 2018

- **Upgrade kits available**
  - SelfServ
    - 6634-K505-V001 IMCRW Track 2 R (Tamper Resistant) upgrade kit
    - 6634-K507-V001 IMCRW Track 3 R (Tamper Resistant) upgrade kit
  - 80 Series
    - 6684-K505-V001 IMCRW Track 2 R (Tamper Resistant) upgrade kit
    - 6684-K507-v001 IMCRW Track 3 R (Tamper Resistant) upgrade kit

- **Encrypted USB communications available**
  - Released as part of APTRA XFS 06.06

**Key Dates – Dip**

- **Feature (F597)**
  - Orderable from 1st Jul 2019 for shipment end August 2019
  - Default from Aug 2019

- **Upgrade kits – currently subject to 14 week leadtime**
  - 6684-K597-V001 Standard Smart Dip to Tamper Resistant Smart Dip Upgrade Kit for 20, 30 & 80 Series (Avail Jun 2019)
  - Also Motorised to Dip conversion kits for select products:
    - 6623-K597-V001 Motorised to Tamper Resistant Smart Dip for SS16, SS22e, SS22 and SS23 only (Avail Jul 2019)
    - 6625-K597-V001 Motorised to Tamper Resistant Smart Dip for SS25, SS26, SS28 only (Avail Jul 2019)

- **Encrypted USB communications available**
  - Released as part of APTRA XFS 06.05
ATM Advanced Card Protection Offer

Protection for Deep Insert Skimming & Eavesdropping Attacks globally

OFFER OVERVIEW

Security solution that addresses the Deep Insert Skimming and Eavesdropping attacks on ATMs that result from constant evolution of card fraud devices utilized by criminals in the market.

WHY THIS OFFER NOW?

In response to the evolution of deep insert skimming devices and eavesdropping attacks, NCR has redesigned both Motorized and Dip card readers, to harden them against these forms of attacks. This offer provides customers the opportunity to enhance the security level of the NCR SelfServ installed base with a plug and play replacement of the card reader with the new Tamper Resistant versions. When used in association with the advanced Skimming Protection Solution (SPS) the new Tamper Resistant Card Reader provides the expanded protection to mitigate against the newest forms of Skimming and Eavesdropping attacks.

OFFER DETAILS

Deep Insert Skimming and Eavesdropping attacks are prevented by replacing the current card readers with the new Tamper Resistant versions. Upgrade kits for Motorized are available now and Dip Card Readers will be orderable by July 2019, while the Dip feature is scheduled to be broken into production during Q3 2019.

Both variants are drop in replacement for existing readers with no SW impact, nor any certification implication. The prices below don't include Installation activity that needs to be agreed at local level based on the replacement information provided with the offer.

Deep Insert Skimming and Eavesdropping Protection Offer

<table>
<thead>
<tr>
<th>Product</th>
<th>PID</th>
<th>Description</th>
<th>Indicative Net Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motorized Tamper Resistant Card Reader</td>
<td>6634-K505-V001 or 6634-K507-V001 or 6684-K505-V001 or 6684-K507-V001</td>
<td>To protect from Deep Insert Skimming and Eavesdropping attacks. Choose appropriate kit based on ATM Model and MRS reader required.</td>
<td>US $500 Based on 75-80% discount from list</td>
</tr>
<tr>
<td>Dip Tamper Resistant Card Reader</td>
<td>6684-K597-V001</td>
<td>To protect from Deep Insert Skimming and Eavesdropping attack.</td>
<td>US $270 Based on 70% discount from list</td>
</tr>
</tbody>
</table>

MARKET AVAILABILITY

- Global Availability

TARGET SEGMENTS

- Targeted for all FI's with NCR Self Serv ATMs.
- Available for Direct Customers and Channel Partners

OFFER TIMEFRAME

- Offer expires End of 2019
Additional Discussion Point with your Customer: Use of Contactless Card Readers as prevention from skimming risks

Vulnerability from the Magnetic Stripe

- Risk remains as long a magnetic strips remain on cards
- EMV, and Chip enabled cards do not solve the problem
- Card skimming still occurs in EMV markets, because the data can be used in non-EMV markets

Contactless Security Benefits

- Eliminates the risk for card data to be skimmed by eliminating the DIP or swipe of the stripe
- Excellent migration properties
- Security does not rely on ‘herd immunity’
- Must use cryptographic capabilities of EMV to gain full benefit
NCR Security Alerts

As part of our commitment to security, we regularly provide alerts and updates to the market on global ATM security issues and situations.

We issue alerts when:

- We receive reports of new attacks
- We receive reports of modifications to attack methods
- Industry compliance issues require actions by ATM deployers

Keep yourself fully informed by signing up today.

response.ncr.com/security-alerts