Identifying, Preventing, and Mitigating Skimming Attacks

April 13, 2016

Sylvia Auyeung – Director, Merchant Risk, Visa Inc.
Lester Chan – Director, Merchant Security, Visa Inc.
Charlie Harrow – Solutions Manager, NCR Corp.
The information or recommendations contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.
Agenda

- Global Data Compromise Landscape
- Liability Shift and Increase in Skimming Attacks
- Card Skimming – Criminal Trends
- Safeguarding Against Skimming Attacks
- How to Report a Skimming Device
- Key Takeaways
- Resources
Global Data Compromise Landscape

Sylvia Auyeung – Director, Merchant Risk, Visa Inc.
Global Data Compromises

- Global data compromise events are slightly higher in 2015 over those managed in 2014
- The U.S. is the largest contributor, mainly due to its large mag stripe infrastructure and an increase in successful attacks on third party service providers
- VE and AP represent the next largest contributors to known breach events, together comprising a quarter of the total
- Breaches in VE and AP are primarily CNP
Global Data Compromises
Breach trends by merchant level

<table>
<thead>
<tr>
<th>Entity Type</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>%</td>
<td>%</td>
<td>%</td>
<td>%</td>
</tr>
<tr>
<td>Level 1</td>
<td>&lt;1%</td>
<td>1%</td>
<td>1%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Level 2</td>
<td>&lt;1%</td>
<td>1%</td>
<td>1%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Level 3</td>
<td>1%</td>
<td>4%</td>
<td>4%</td>
<td>5%</td>
</tr>
<tr>
<td>Level 4</td>
<td>95%</td>
<td>92%</td>
<td>93%</td>
<td>92%</td>
</tr>
<tr>
<td>Agent</td>
<td>&lt;1%</td>
<td>1%</td>
<td>1%</td>
<td>2%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
<td>&lt;1%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Large breach events (levels 1 & 2)

- As a proportion of the total number of breach events, L4s remain the vast majority of compromise cases (93% in 2014-2015)
- At-risk accounts in 2015 were largely attributed to L4 merchants
- Level 4 merchants outnumber L1s in the US

- Fewer level 1 and 2 breaches in 2015
- Threat actors are targeting smaller interconnected merchants in large numbers
- Restaurants and “other retail” make up the biggest portion of total known breaches
- Quick service restaurants, supermarkets, and lodging make up the other top MCCs
EMV Liability Shift and Increase in Skimming Attacks

Lester Chan – Director, Merchant Security, Visa Inc.
EMV Liability Shift and Counterfeit Fraud

Understanding how the liability shift affects fraud

Oct. 2015 U.S. EMV liability shift (excludes AFD & ATM)

Criminals continue to attack the Payment System to steal and monetize cardholder data

Oct. 2017 U.S. AFD & ATM liability shift
EMV Chip Adoption & Fraud

Fraud will likely migrate to other channels

![Graph showing the relationship between EMV chip adoption, CNP fraud, and counterfeit fraud with a liability shift point.](image)
Fraud Migration to Other Channels
Fraud migrating to e-commerce, automated fuel dispensers, and ATMs

- Fraud and attacks will continue in CNP/e-commerce channels
- Insecure websites and mis-configured security settings
- Internet facing websites getting exploited

- Scan for vulnerabilities
- Be aware of OWASP Top 10
- Work with a qualified integrator/reseller

- AFD EMV liability shift in October 2017
- Stations in remote locations often targeted
- Skimmers and overlays are getting more sophisticated

- Regularly check pumps for devices
- Review POS for overlays
- Know who to contact if known or suspected attack

- ATM EMV liability shift in October 2017
- Overlays and cameras are getting more sophisticated
- Remote locations at higher risk

- Regularly check ATMs
- Ensure software is kept up to date
- Know who to contact if known or suspected attack
Rise in Skimming Attacks
Criminals are targeting mag stripe data

• Criminals are shifting their attacks to skimming
• Increase skimming attacks in the news
• Criminals are targeting:
  – Self-checkout terminals at stores
  – Automated fuel dispensers
  – White-label ATMs
• Increasing in sophistication of attacks and technology
Card Skimming – Criminal Trends

Charlie Harrow – Solutions Manager, NCR Corp.
Card Skimming: Trends

Skimming continues to be the #1 cause of fraud loss on ATMs.

- Criminal techniques have grown increasingly sophisticated
- Criminal techniques have diversified to avoid anti-skimming defences
- An arms race has taken place
  - Industrialisation
  - Avoidance techniques
  - Sabotage
  - Side Channels
“Traditional” Skimming Attack

Skimmer added to fake panel over card slot.
Camera concealed in fake panel above PIN Pad.
Skimming History: full fascia overlays…
Getting smaller….
Getting smaller…. 
Six small batteries connected to micro switches

Transmitter Circuit

Micro Switches

Magnetic Read Head

Transmitter Antenna

Smaller....
Smallest: Insert Skimmer, Germany
Bypassing Passive Protection
Bezel Overlay Skimmer - Canada
Bulgaria
Skimming - Ireland
Skimming - Ireland
Skimming – UK
Australia
Insert Skimmers
Criminal Lab Raid: Germany

Card Reader Moulds and Surrounds
Bypassing Active Prevention
Fascia penetration

Switzerland
Ireland – Internal Attacks
Eavesdropping attacks expanding

- Create hole in Fascia, typically under card orientation window
- Attach to control electronics within card reader module
- Fascia break-through “naturally” hidden
- Impact as per “traditional” skimming
- Different styles of eavesdropping device observed.
Eavesdropping - Global Expansion

- Attacks continuing globally

UK

Canada
Mexico – Internal Skimming: DIP
“Deep” Insert Skimming

- 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 often transmit card data in real time, no on board storage
Deep Insert Skimmers - Variations

- New form factor Deep Insert Skimmers reported in Turkey and Ireland (not pictured).
Sabotage: Attempts to Disable SPS

- Criminal has attempted a crude attack on the SPS bezel to damage and disable the SPS electromagnetic disruptor.

- SPS anti-tamper sensors will detect and alert on a wide range of tamper conditions, including simple disabling attacks like this one.

- ATM infrastructure MUST be configured to react to SPS anti-tamper alerts.
Attacks concerning CPK

Sabotage

Cloning
Software Skimming: Offline Malware Attack

- Insert to Card Reader
- Connector turned through 90 deg.
- Connects to Card Reader USB Connections
- Malware harvests Card and PIN Data
- Allows injection of malware ‘from the street’
- Exploits non-PCI EPP firmware

1. Direction of inserting the fraud device into the reader
2. After inserting the fraud device into the reader, turn this handle clock-wise over 90 degree
3. By turning the handle clock-wise over 90 degree, the USB connector is rotated to a more vertical position

- Top of device
Network Sniffing: Internal and External

- Sniffing device connects inline with network cable
- Device is able to intercept and read all network traffic, including card data.
- A separate device is used to capture the PIN. Both overlays and cameras have been observed
- PIN capture device transmits the PIN to the sniffer
- Encrypted communications prevents this attack
‘Shimming’ - Mexico, Greece, Portugal

- Correct EMV implementation protects against this attack
Bluetooth Skimming

- Blog posts report internal skimming in Mexico
- Bluetooth devices transmit card and PIN data from inside the ATM.
- Bugs placed inside card reader and EPP
- High levels of corruption of service staff
- Attacks are not possible with latest EPPs
- Attacks highlight the importance of EPP Key Management

---

Bluetooth Skimming in Mexico

Summary

NCR is aware of the recent blog reports of Bluetooth Skimming in Mexico, and we would offer the following commentary.

The attack MO is described as consisting of electronic devices that are installed inside the ATM that are capable of capturing card data and PIN data, and then using Bluetooth technology to transmit the data to the attacker. With the fraudulent devices on the inside of the ATM, there are no visible signs for the ATM user to know that skimming devices have been installed.

The critical factor to the success of this crime is the ability of the criminal to insert a PIN capturing device inside the ATM PIN pad. This is not possible on a modern NCR ATM equipped with a PCI compliant Encrypting PIN Pad. No NCR ATMs were involved in the Mexico fraud so we cannot comment on the specific technology that was compromised in those attacks. However, if an NCR EPP is disassembled in any way, any sensitive data within the device is immediately erased and the device is rendered permanently inoperable, as per PCI requirements.

Guidance and Recommendations:

- Deploy only PCI compliant EPPs running PCI compliant firmware. NCR EPPs are designed such that it is infeasible for malware or internal lapses to gain access to a plain text PIN.
- Ensure that key loading procedures meet the security requirements of ISO 11568 and/or ANSI X9.24. Initial key loading is a sensitive function and must be treated accordingly. The EPP serial number must be verified as the expected serial number prior to loading any cryptographic keys. If an ATM service call necessitates a swap of the EPP, then the service call must be validated before cryptographic keys are loaded into the new device.
- Use Remote Key Management as the method of key loading rather than manual key loading. Remote Key Management means EPP cryptographic keys are transferred directly from the Host Security Module to the EPP in encrypted format, such that no individual will have access to the key.
- If manual key loading methods are employed, key loading procedures that comply with ISO 11568 and/or ANSI X9.24 must exist and be followed to ensure the secrecy of the keys. Regular audits should be performed to ensure the procedures are followed. Audits should follow ANSI TR30 or PCI PIN.
- Ensure that ATM cabinet is appropriately secured. Prevent unauthorised personnel from accessing the interior of the ATM cabinet where they could tamper with the ATM controller or add ‘hacking’ equipment. This is particularly appropriate to free standing ATMs in unsupervised locations.

© 2015 NCR Corporation. All rights reserved.
Stereo Skimming

- Two confirmed reports of stereo skimming in Ireland
- ATMs were fitted with TMD CPK 6000 which failed to prevent the attacks.
- Stereo skimming uses 2 separate skimmers wired in differential mode to eliminate the effects of electromagnetic jamming
- Stereo skimming is very hard to defend against using only electromagnetic jamming
- NCR recommend using skimmer detect functionality in parallel with electromagnetic jamming
## Card Skimming - Threat Summary

<table>
<thead>
<tr>
<th>Skimming Category</th>
<th>Description</th>
<th>Recommended Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bezel Overlay</td>
<td>Manufactured overlay containing a skimmer which fits a specific ATM model</td>
<td>SPS with Skimmer Detect and Alert Monitoring</td>
</tr>
<tr>
<td>Bezel Insert</td>
<td>Manufactured insert containing a skimmer which fits a specific ATM model</td>
<td>SPS with Skimmer Detect and Alert Monitoring</td>
</tr>
<tr>
<td>Card Read Tap - Destructive</td>
<td>Attacks that penetrate the ATM fascia or cabinet with the intention of providing direct access to the card reader</td>
<td>SPS with Skimmer Detect and Alert Monitoring, plus Anti-Eavesdropping Kit</td>
</tr>
<tr>
<td>Card Read Tap - Non-Destructive</td>
<td>Attacks that involve opening the ATM cabinet with the intention of providing direct access to the card reader</td>
<td>ATM location security, appropriate cabinet locks, encrypted USB</td>
</tr>
<tr>
<td>Differential Skimming (Stereo Skimming)</td>
<td>Using twin read heads connected in differential mode to negate the effects of a jamming signal</td>
<td>SPS with Skimmer Detect and Alert Monitoring</td>
</tr>
<tr>
<td>Deep Insert Skimmer</td>
<td>A device placed inside the card reader using the card slot as the entry point</td>
<td>Card reader device detection firmware, anti-insert kit</td>
</tr>
<tr>
<td>Sabotage</td>
<td>Any attempt to disable any anti-skimming technology</td>
<td>SPS with Skimmer Detect and Alert Monitoring</td>
</tr>
<tr>
<td>Shimming</td>
<td>Capture of chip card data with the intent to produce a cloned mag strip card</td>
<td>Transaction Authorisation as per EMV</td>
</tr>
<tr>
<td>Network Sniffing</td>
<td>Capture of card data via sniffing of network communications to the host</td>
<td>Communications Encryption TLS 1.2</td>
</tr>
</tbody>
</table>
PIN capture: Keyboard Overlays

Keyboard overlays increase work function for criminal - cost/effort
Overlays have a higher probability of discovery
Typically cameras are used to capture PINs
SelfServ key design a small advantage
PIN Pad Overlay - Mexico

EPP overlay created by slicing the top from a genuine NCR PIN pad.

Device fitted ‘correctly’ into the ATM, with original ATM PIN pad directly below it.

Attacker required access into top box to fit the overlay.
PIN capture: Cameras......
PIN capture: Shoulder Surfing

The gentleman on the left demonstrates the old fashioned way to capture a PIN…….
Safeguarding Against Skimming Attacks

Charlie Harrow – Solutions Manager, NCR Corp.
Three effective strategies to combat skimming

<table>
<thead>
<tr>
<th>Migrate from magnetic stripe</th>
<th>Protect the installed base</th>
<th>Identify anomalous behaviour</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Reduce the counterfeit card risk</td>
<td>▪ While mag stripe is still used, we need effective, active, defended, prevention and detection tools</td>
<td>▪ If the worst happens and cards are skimmed, we must limit the opportunity for the data to be used</td>
</tr>
<tr>
<td>▪ Migrate to EMV chip</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If the worst happens and cards are skimmed, we must limit the opportunity for the data to be used.
Use of Contactless Card Readers as prevention from skimming risks

Magnetic Stripe Vulnerabilities
- Markets that use magnetic stripe are more vulnerable to counterfeit
- EMV chip cards reduce the risk
- 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
- Just one solution reduce the risk
Contactless EMV live today

In November 2014, ANZ announced a world-first ATM EMV transaction: ‘Tap & PIN’

ANZ claims ‘world’s safest ATM’ source .. source Australian Banking and Finance
ANZ to roll out tap and PIN ATM in 2015 .. source ZDnet

- Faster Transaction
- Secure Contactless Transaction
- Seen as a good way to avoid skimming
- Mobile phone and ATM can communicate in a secure way
Active Anti-Card Skimming

- Prevents skimming through object detection and electromagnetic disruption
- Built in self defence using multiple anti-tamper sensors
- Integration into ATM Software to provide flexible response to attack
- Peripheral defences to prevent side channel attacks

QUICK FACTS

- Optimum protection for NCR ATMS
- Comprehensive levels of anti-tamper defences
- Upgrade kit availability
- Supported through NCR normal support channels
- Available for Motorized and DIP Card readers
- Downloadable software for ease of flexible response
Transaction Processing and Fraud Detection

- ACQUIRE
- SWITCH/ROUTE
- AUTHORISE

Other Channel Systems

ASSIGN TO CARD NETWORKS AND NATIONAL NETWORKS

MODEL DETECTION
RULES DETECTION
ALERT/ACTION
INVESTIGATION

FRACTALS (Enterprise Fraud Detection)
FINALLY - NCR SECURITY ALERTS
Are you enrolled?

- NCR have a proven set of solutions and practice recommendations to reduce your risk

- Get on NCR's Alert List
  - Notification of new attacks response.ncr.com/security-alerts

- Lock down your BIOS
How to Report a Skimming Device

Lester Chan – Director, Merchant Security, Visa Inc.
Best Practices on Handling and Reporting

What to do if a skimmer is found

Do not approach or confront anyone who looks suspicious
Might be installing or removing a skimming device
May be armed and dangerous

Document and take pictures of the skimming device as-is
Document before and after removal
Document date/time

Use protective gloves to remove the device
Criminals may leave DNA on device
Keep in protective bag and store securely
Review CCTV for surveillance of suspects

Contact the local authorities and the U.S. Secret Service
U.S. Secret Service is the law enforcement branch responsible for investigating these crimes
Know how to report compromises to Visa

Know how to report compromises to Visa
How to Report a Compromise to Visa
Reporting requirements after a skimmer is found Issuers (ATMs)

Review Compromised Guidelines

<table>
<thead>
<tr>
<th>What To Do If Compromised</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visa Inc. Fraud Investigation Procedures</td>
</tr>
<tr>
<td>Version 4.0 (Global)</td>
</tr>
<tr>
<td>Effective September 2013</td>
</tr>
<tr>
<td>Visa Public</td>
</tr>
</tbody>
</table>

Complete Questionnaire

Send to: USFraudControl@Visa.com

1. Send Questionnaire to Visa Cyber Investigations with incident details
2. Try to determine the potential Window of Exposure of the event
3. Pull and send in compromised accounts to Visa via CAMS*
4. Visa will distribute the at-risk accounts to the affected Issuers via CAMS

*Note – Most Issuers are set up as CAMS receivers only, send email to VAA_VRM@Visa.com to be a submitter
How to Report a Compromise to Visa

Review Compromised Guidelines

What To Do If Compromised
Visa Inc. Fraud Investigation Procedures
Version 4.0 (Global)
Effective September 2013
Visa Public

Complete Questionnaire

Send to acquirer

1. Acquirer will forward questionnaire to Visa Cyber Investigations with incident details
2. Skimming incidents often involve the compromise of highly sensitive PIN data
3. Issuers need to be notified of the potential at-risk accounts quickly
4. Merchants should try to determine the potential Window of Exposure of the event
5. Acquirers should pull and send in the compromised accounts to Visa via CAMS
6. Visa will distribute the at-risk accounts to the affected Issuers via CAMS
Key Takeaways

- Be aware that due to EMV liability shift, fraud and compromises will likely migrate
- Recognize that criminals are targeting mag stripe data and transactions
- Skimming devices are becoming more sophisticated
- Understand how to identify different types of skimming devices
- Learn best practices for safeguarding against skimming attacks
- Conduct regular, ongoing training for current and new employees
- Know what to do if a skimmer is found and how to report a suspected compromise
Upcoming Events and Resources

Resources

- PCI Standards Council: Skimming Prevention
- NCR Security Alerts: response.ncr.com/security-alerts
- Visa’s “What To Do If Compromised” guidelines
- Visa’s “Payment Acceptance Best Practices for U.S. Retail Petroleum Merchants” guidelines

Upcoming Webinars – Training page on www.visa.com/cisp
- Changes to PCI DSS 3.2 – May 11, 2016 - Janet Cookson, Director, Security Standards, Visa Inc.

Visa Data Security Website – www.visa.com/cisp
- Alerts, Bulletins
- Best Practices, White Papers
- Webinars

PCI Security Standards Council Website – www.pcissc.org
- Data Security Standards – PCI DSS, PA-DSS, PTS
- Programs – ASV, ISA, PA-QSA, PFI, PTS, QSA, QIR, PCIP, and P2PE
- Fact Sheets – ATM Security, Mobile Payments Acceptance, Tokenization, Cloud Computing, and many more...
Questions?