

Threat Landscape: Skimming at the Point of Sale



Tia D. Ilori, Sr. Director, Visa, Global Fraud & Breach Investigations
Chris Forsythe, Sr. Risk Analyst, Visa, Payment Fraud Disruption & Intelligence

28 June 2016

Disclaimer

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
- Modus Operandi of a Typical Skimming Attack
- Safeguarding Against Skimming
- Detecting, Responding and Reporting a Skimming Incident
- Key Takeaways

A dark blue background featuring a faint, stylized image of the Golden Gate Bridge at night, with its towers and suspension cables visible against a dark sky. The bridge's lights are represented by small white dots.

Global Data Compromise Landscape

Tia D. Ilori
Senior Director, Global Fraud and Breach Investigations
Visa Inc.



Visa Security Pillars

Remove sensitive data



Devalue Data

Render data useless for criminals, reducing incentive for payment breaches

- Tokenization
- EMV



Protect Data

Safeguard payment data

- Encryption
- PCI DSS

Prevent fraud



Harness Data

Identify fraud before it occurs and increase confidence in approving good transactions

- Risk-Based Authentication
- One-time Passcode
- Dynamic CVV2
- Breach Response



Empower Consumers

Engage cardholders as an underutilized resource in fighting fraud

- Transaction Alerts
- Spend Controls
- Geolocation

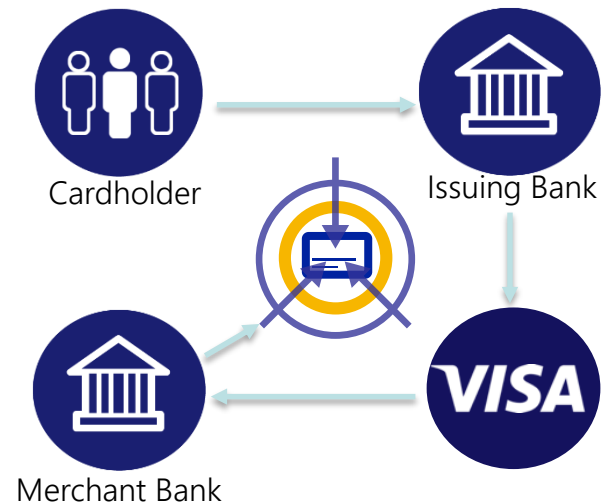
Transactional Threat Intelligence

Intelligence comes from recognizing fraud patterns, predicting fraud activity

- Cardholders report fraud to their bank
- Banks report fraud to Visa (CPP)
- Visa reports fraud to other banks
- Breach found, stopped

One major limitation: **What if there's no fraud?**

Breach Detection Cycle

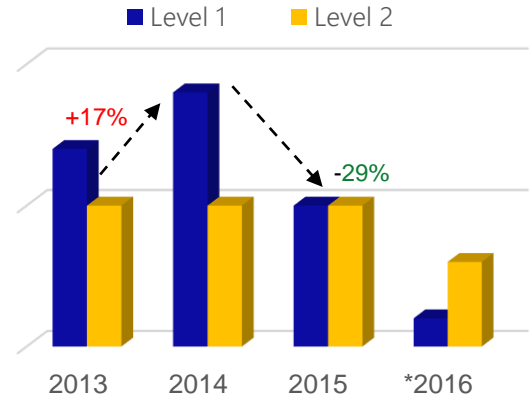


Global Fraud and Breach Investigation Trends

Breach Events by Entity Type and Merchant Level

| Entity Type | 2013 | 2014 | 2015 | 2016* |
|----------------|-------------|-------------|-------------|-------------|
| | % | % | % | % |
| Level 1 | 1% | 1% | <1% | 0% |
| Level 2 | 1% | 1% | <1% | 1% |
| Level 3 | 4% | 4% | 5% | 9% |
| Level 4 | 92% | 93% | 91% | 87% |
| Agent | 1% | 1% | 3% | 2% |
| Other | <1% | 0% | 0% | 0% |
| Total | 100% | 100% | 100% | 100% |

- As a proportion of the total number of breach events, Level 4 (L4) merchants represent 90% of compromise cases investigated in 2015
- Nearly half of the at-risk accounts distributed through CAMS in 2015 were attributed to L4 merchants
- Small merchant compromises are fueled by use of insecure Integrator/Resellers
- Threat actors continue to target smaller interconnected merchants in large numbers

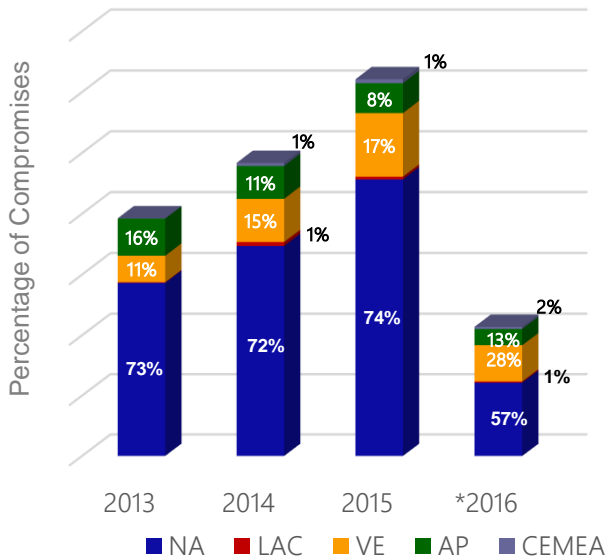


- Visa investigated fewer large merchant breaches in 2015; Down 29% from 2014
 - However, skimming attacks across the grocer and retail verticals are on the rise
- U.S. large breaches comprised 53% of the total at-risk accounts distributed in 2015 – related to large hotel and restaurant events

*2016 year-to-date through May
Source: Compromised Account Management System (CAMS) – Original "IC" and "PA" Alerts

Global CAMS Distribution

Compromise Account Management System (CAMS) - Alerts Distributed by Region



- In 2015, total CAMS alerts increased to the highest level in 3 years
- The sheer magnitude of the number of small merchants worldwide, especially in the United States, comprise the majority of reported compromises
- Investigations revealed cyber criminals exploiting inadequate controls to gain unauthorized access to the POS systems of small level 4 merchants and then ultimately to their payment card data

*2016 year-to-date through May

Source: Compromised Account Management System (CAMS) – Original “IC” and “PA” Alerts

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
- Attackers will exploit insecure websites and mis-configured security settings
- Internet facing websites at-risk

- Scan for vulnerabilities
- Be aware of OWASP Top 10



- AFD EMV liability shift in October 2017
- Stations in remote locations often targeted
- Skimmers and overlays more sophisticated and harder to detect

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



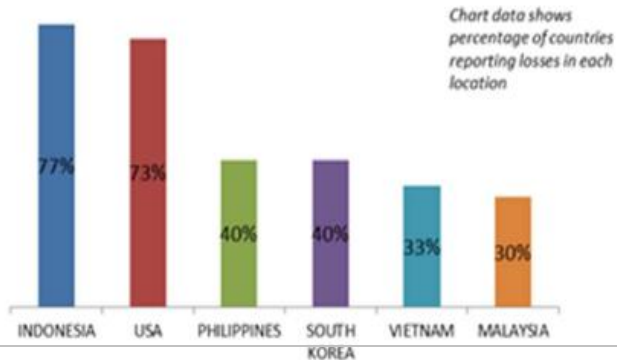
- ATM EMV liability shift in October 2017
- Overlays and cameras are more sophisticated
- Remote locations at higher risk

- Regularly check ATMs
- Ensure software is kept up to date
- Know who to contact if known or suspected attack

Card Skimming: ATM Trends

ATM Related Skimming losses - Top 6 Locations

(As reported by 17 Countries at 36th EAST Meeting)



Source: European ATM Security Team (EAST)

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

- Criminal techniques have grown increasingly sophisticated and diversified to avoid anti-skimming defenses
- An arms race:
 - Industrialization
 - Avoidance techniques
 - Sabotage
 - Side Channels

Rise in Skimming Attacks

Criminals are targeting mag stripe data

- Criminals are shifting their attacks to skimming
- Increase in report skimming attacks in the news
- Criminals are targeting:
 - Self-checkout terminals
 - Automated fuel dispensers
 - White-label ATMs
- Increasing in sophistication of attacks and technology
- All stores targeted – regardless if they are 100% EMV enabled
- Skimming Overlays
 - 3D printers leveraged by criminals
 - Placed in seconds not minutes as with physical swaps
 - Easier to deploy in large numbers

The screenshot shows a news article from The Wall Street Journal. The main headline is "Skimming devices found at two gas stations". Below it, a sub-headline reads "Skimming devices now popping up at grocery stores". The article is by Cheri Hardmon, dated Friday, February 21, 2016. A photograph shows a person's hand using a blue skimming device on a credit card terminal. A "CONSUMER ALERT" banner at the bottom of the photo reads "GROCERY STORE CREDIT CARD SKIMMERS". The article text mentions that a man was arrested for second-degree felony credit card skimming in Calhoun County, and that the Department of Agriculture routinely evaluates gasoline stations, with one example being a station on Popps South at 763 River Ave. The article also includes a "TRENDING" section with a link to a story about a man arrested for second-degree felony credit card skimming.

Modus Operandi of a Typical Skimming Attack

Chris Forsythe
Senior Risk Analyst, Payment Fraud Disruption and Intelligence Visa
Inc.



Modus Operandi of a Typical Attack

- Suspects will operate in groups of 2 to 3
 - 1st suspect places device
 - 2nd suspect provides cover - shielding any view of the device placement; may utilize large items at checkout
 - 3rd suspect acts as lookout and providing counter surveillance
 - Suspects may scout a location prior to placing a device so be aware of individuals that appear out of place
- Targeted terminals include:
 - Self checkout lanes
 - Coffee stands
 - Deli counters
 - Regularly unattended devices



[Skimmers Caught on Tape \(Video\)](#)

Overlay Examples



Criminal Lab Raid: Germany





Safeguarding Against Skimming



Device Inventory Management

- Daily checks of POS terminals
 - Use teams when inspecting devices
- Maintain a log of devices and their locations within the business
- Use unique markings/stickers on your devices to quickly identify overlays
- Utilize tamper screws or cable locks
- Identify key risk areas where attacks may occur
 - High volume
 - Unattended
 - Areas with limited visibility

Use of Contactless Card Readers to Minimize 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

- Reduces the risk for card data to be skimmed since there is no dip or swipe
- Excellent migration properties
- Just one solution reduce the risk

Always Use PCI Approved Devices

- Follow Visa deployment requirements for use of *only* PCI approved PIN Entry Devices
- As a best practice:
 - Use only PCI approved Unattended Payment Terminals (UPT)
 - Use devices that are PCI approved for Secure Reading and Exchange of Data (SRED)
- Switch to EMV terminals
- Monitor for changes to internal serial numbers of devices
- Monitor for connectivity changes



Detecting, Responding and Reporting a Skimming Incident



Responding to a Skimming Incident

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.S.S.)
- U.S.S.S is the law enforcement branch responsible for investigating these crimes
- Notify your acquirer who will coordinate the investigation with Visa

How to Report a Compromise to Visa

Review Compromised Guidelines

Complete Questionnaire

Send to Visa / Acquirer

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

Key Point to Remember

The information required below is applicable to suspected/confirmed compromised entities such as Visa clients or members, merchants, processors, or third-party service providers.

Entity Information

| Description | Response |
|---|----------|
| Name of entity | |
| Is entity a direct-connect to Visa? | |
| If entity is a merchant, provide the Merchant Category Code (MCC) | |
| Acquirer BIN | |

1. Complete Incident Questionnaire
 - Issuers send to Visa Fraud and Breach Investigations
 - Merchants send to Acquirer (who will forward to Visa)
2. Skimming incidents often involve the compromise of **highly sensitive PIN data**
3. Issuers must be notified of the potential at-risk accounts quickly
4. Try to determine the potential Window of Exposure of the event
5. Pulling at-risk accounts
 - Issuers pull and send compromised accounts to Visa via CAMS*
 - Acquirers pull and send in the compromised accounts on behalf of the merchant via CAMS
6. 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

Key Takeaways



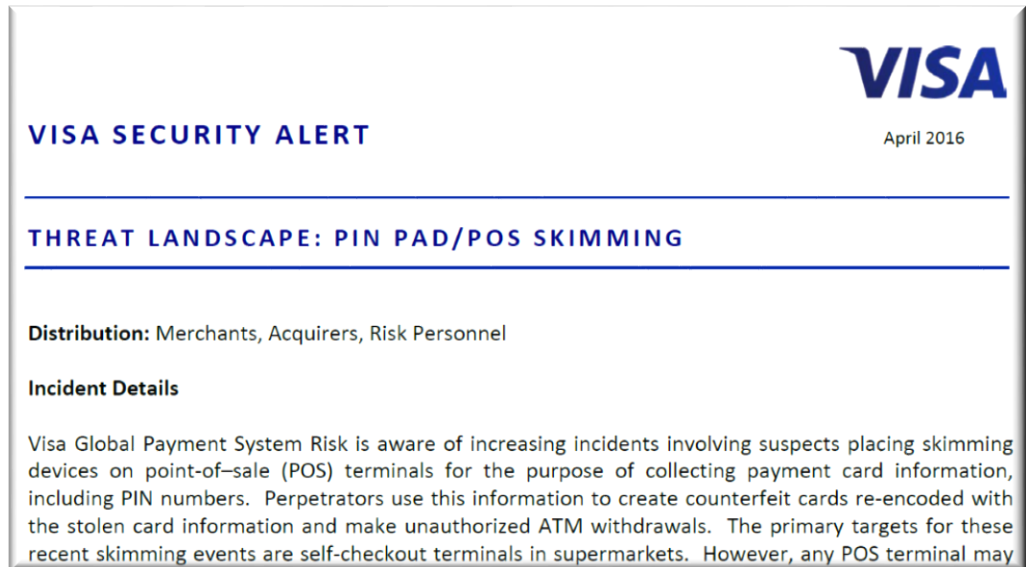
Conclusion and Recap: What to Expect

- Be aware that due to EMV liability shift, fraud and compromises will likely migrate to other channels ...
- Recognize that criminals are targeting mag stripe data and transactions
- Skimming devices are becoming more sophisticated
- Increase inspections and 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
- These attacks are not limited to instore devices; Check Kiosk and ATMs
- Key to mitigating and preventing additional data loss is having a strong response plan in place

Visa Security Alerts

Information on the latest Skimming Attacks

Visit www.visa.com/cisp for recent Skimming Security Alerts from Visa



The image shows a document header for a Visa Security Alert. The Visa logo is in the top right corner. The main title is 'VISA SECURITY ALERT' in blue, with the date 'April 2016' to its right. Below this is a horizontal line, followed by the subtitle 'THREAT LANDSCAPE: PIN PAD/POS SKIMMING' in blue, also followed by a horizontal line. The text 'Distribution: Merchants, Acquirers, Risk Personnel' is listed below. Under the heading 'Incident Details', a paragraph describes the threat: 'Visa Global Payment System Risk is aware of increasing incidents involving suspects placing skimming devices on point-of-sale (POS) terminals for the purpose of collecting payment card information, including PIN numbers. Perpetrators use this information to create counterfeit cards re-encoded with the stolen card information and make unauthorized ATM withdrawals. The primary targets for these recent skimming events are self-checkout terminals in supermarkets. However, any POS terminal may'.

Upcoming Events and Resources

Resources

- PCI Standards Council: [Skimming Prevention](#)
- Visa's "[What To Do If Compromised](#)" guidelines
- Visa's "[Payment Acceptance Best Practices for U.S. Retail Petroleum Merchants](#)" guidelines

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?



VISA