Webinar - Skimming and Fraud Protection for Petroleum Merchants

November 14th 2013

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.

Skimming and Fraud Protection for Petroleum Merchants Webinar

Skimming at the AFD

Mario Rivero, Jr
Business Leader, Visa Inc.
November 14, 2013
Visa Public

What to do if a skimmer is detected

- Notify Corporate office, Franchisor or Distributor
- Local Law Enforcement or US Secret Service field office
- Notify Retailer's Acquiring Bank or Processor
- Contact Visa Fraud Investigations at: usfraudcontrol@visa.com
- Provide Visa a summary of event:
    1. Date, time & how it was discovered
    2. Provide photograph of device and installation
    3. Time frame device was installed
    4. Provide accounts processed thru the tampered AFD during time frame
- Visa will distribute at risk accounts to Issuers to prevent fraudulent use and minimize impact

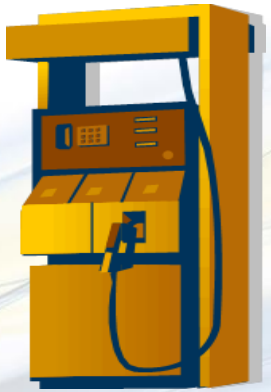
Dealers must have documented notification procedures before an event occurs…

Practices to minimize the risk of a data compromise

- Ensure entry and access to AFDs is limited to specific employees according to job functions
- Schedule frequent inspections of AFDs
- Train staff on what interior of AFD should look like
- Ensure AFD access keys are not shared among large numbers of devices and are securely managed
- Verify that AFD and POS PED access is restricted to designated employees and service technicians
- Use CCTV video cameras to monitor and deter
- Work with Vendors to upgrade equipment and anti-tampering tools

Monitoring Suspicious Activity

- Single customer activating multiple AFDs
- Filling multiple vehicles from one AFD
- Filling large non-commercial vehicle containers
- Fueling several times a day (location and chain-wide)
- “Using” several cards without dispensing fuel (testing)
- Individuals offering to use their card to pump fuels for customers in exchange for cash



Skimming and Fraud Protection for Petroleum Merchants – Securing PIN Acceptance

November 14, 2013

Stoddard Lambertson
Payment System Security
Visa Inc.

Note: This presentation will be posted on www.visa.com/cisp

Agenda

- Compliant PIN-Entry Device (PED) Acquisitions
- Expiration of PCI Approved Devices V1.X
- Visa mandates for PED usage
- Best Practices for PED Acquisitions
- Visa's new PIN Security Compliance Framework

PIN Entry Device (PED) Testing

- PCI Security Standards Council (SSC) manages and approves laboratories for testing PEDs and PED approvals
- Visa started program in 2002 (Pre-PCI PEDs)
- Adopted by PCI SSC in 2007
- Testing consists of verification of the Hardware, ***Firmware*** and TDES capability
- Separate processes for the evaluation of device types – POS, Encrypting PIN PAD etc.
- www.pcisecuritystandards.org/pin
- Visa has mandates for the purchasing, use and deployment of PCI-Approved PEDs

Compliant U.S. AFD EPP Acquisitions

Effective January 1, 2009 - all newly deployed U.S. AFDs must have a PCI approved Encrypting PIN Pad (EPP)

- Ensure newly purchased EPPs are PCI-approved and listed on the PCI Approved Device List…***and not expired***
- PIN Security Requirements enforced via *Visa International Operating Regulations* ID#: 151013-100512-0027086
- **Develop EPP purchase policies to:**
  - Never purchase expired EPPs – Version 1.X PEDs Expire April 2014
  - Ensure that ***both*** the EPP and the firmware are PCI approved

  Best Practices:
  - Attempt to purchase the highest version of PCI approved EPPs – currently some Vendors are testing PEDs against Version 4.X
  - Include language in purchase agreement that binds manufacturer or reseller to supply only PCI approved EPPs
  - Attach the relevant section of the PCI Approved Device List to the purchase contract
  - Purchase EPP versions that support EMV upgrades
  - Attempt to purchase and deploy PCI Unattended Payment Terminal (UPT) approved devices

PCI Approved Unattended Payment Terminals – UPT

Currently 16 UPT devices listed and approved

Class of cardholder-operated payment devices that read, capture and transmit card information in conjunction with an unattended self-service device:

1. Automated Fuel Dispensers
2. Ticketing Machines / Vending Machines / Kiosks

UPTs may have a compound architecture directly combining payment and the delivery of services and/or goods

- PIN support
- Prompt control
- Key management
- PIN-entry technology

- Use of PCI Approved UPTs is a Best Practice
- Use of PCI Approved EPPs is required

PCI PIN Transaction Security Devices

- Always validate Hardware, Firmware and Application prior to purchase

PCI Security Standards Council

Home · Contact · FAQs · Change Your Language · Search

For Merchants | PCI Standards & Documents | Approved Companies & Providers | Training | News & Events | About Us | Get Involved

ofessionals & Services · Approved Companies & Providers · Approved PIN Transaction Security Devices Text size · Share · Print

- Overview
- Verify QSA Employee
- Qualified Security Assessors (QSA)
- Payment Application QSAs (PA-QSA)
- Approved Scanning Vendors (ASV)
- Verify a PCIP
- Approved PIN Transaction Security
- Validated Payment Applications
- Validated P2PE Solutions
- Validated P2PE Applications
- Internal Security Assessors (ISA)
- Verify an ISA
- PCI Forensic Investigator (PFI)
- PCI Point-to-Point Encryption (P2PE)
- Qualified Integrators and Resellers
- QSA Remediation Statement
- Become Qualified
- Merchant Feedback Forms

Approved PIN Transaction Security Devices

www.pcisecuritystandards.org

· Export

Please review the legal conditions and restrictions regarding PCI PTS approval contained in the **Payment Card Industry PIN Transaction Security Testing and Approval Program Guide**.

PCI Security Standards Council bulletin on determination of PCI approval status for PTS devices
Payment Card Industry (PCI) Recognized Laboratories
Derived Test Requirements

Additional PIN Transaction Security (PTS) documents are available in the **document library**.

Search by Company Name, Product Name, Approval Number, Product Type, Version or Expiration Date, Functions Provided.

Product Type: UPT — Search — Clear

PIN Acceptance Devices | Non PED | HSM | SCR

Results: 16 — Page: 1

Company	Approval Number	Version	Product Type	Expiry Date
Cryptera A/S				
www.cryptera.com				
iNT 7000				
Hardware #: xxx-3310-62xx R2x (online&offline), xxx-3310-62xx R1x (online only) **Firmware #:** 414-0580 R2x (online & offline), 414 -0580 R1x (online only) **Applic #:**	4-20190	1.x	UPT	30 Apr 2017
Gilbarco s.r.l.				

POS PED Categories and Usage

Non Lab-Evaluated / Non Visa Approved

Attended PEDs
- Deployed prior to Jan. 2004
- Mandatory Visa sunset date July 2010

US AFD PEDs
- No Visa Inc. sunset date
- No new deployments

Pre-PCI Approved PEDs

Attended PEDs
- Deployed after Jan. 2004
- Expired on Dec. 2007
- Visa sunset date Dec. 2014
- Listed by Visa - visa.com/cisp

US AFD PEDs
- No Visa Inc. sunset date*
- No new deployments

PCI Approved PEDs

Attended PEDs
- Deployed after Dec. 2007
- V1.X PEDs expire April 2014 – purchases not allowed
- No Visa Inc. sunset date
- Listed by PCI SSC

US AFD PEDs
- EPPs deployed since Jan. 2009
- No Visa Inc. sunset date*
- Listed by PCI SSC

Best Practices for POS PED Acquisitions:

- **Locate PED on PCI SSC website to validate approval status**
- **Keep print screen of PCI PED approval with PO**
- **Purchase the latest version of PCI PEDs when possible – V4**

***NOTE: Visa Europe requires *all* Unattended pre-PCI and PCI V1.X PEDs be replaced by December 2020**
For more information contact: visaeuropepin@visa.com

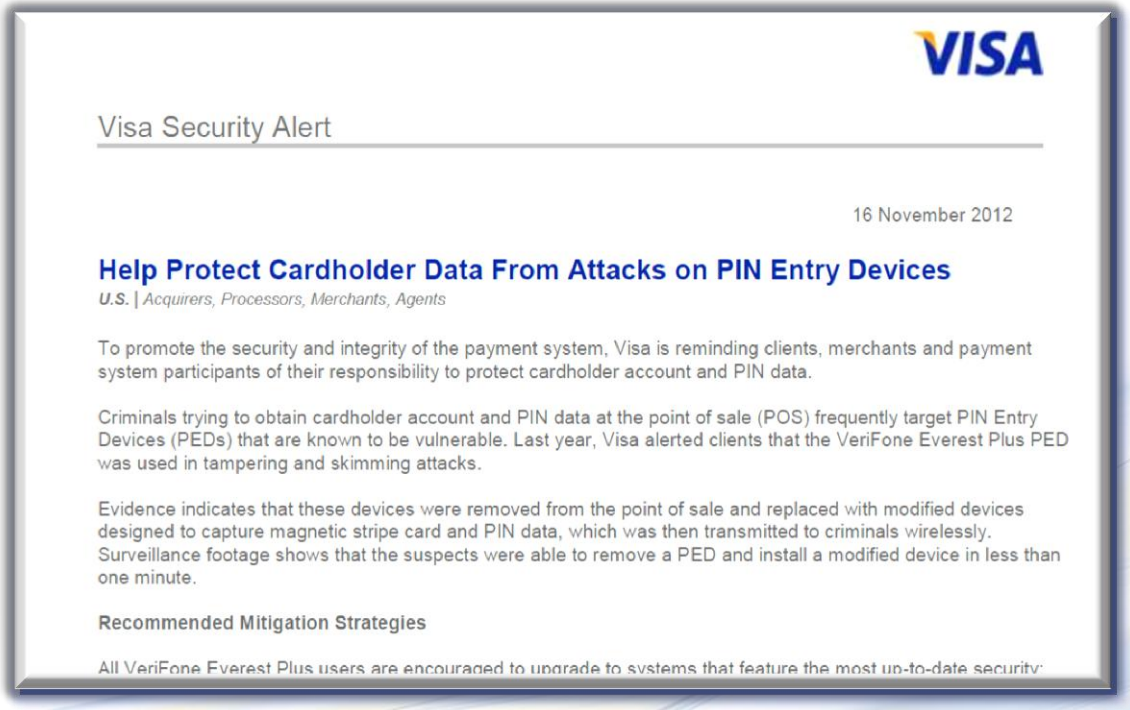
Visa What to Do If Compromised

- New notification requirements for PIN Entry Device (PED) attacks
- If PCI PTS Approved device is suspected, compromised entity must provide Vendor the with all relevant information
- Vendors that manufacture PCI PTS Approved PEDs are required to inform the PCI Security Standards Council
- Includes attended POS PEDs or Encrypting PIN PADs (EPPs) deployed at the AFD
- Some of the PEDs may be sent to the Vendor for inspection
- PCI SSC may de-list the PED based on analysis of Vendor provided reporting

www.visa.com/cisp

Compromised PIN-Entry Device List

- Review PEDs in use to identify any known vulnerable devices
- *Visa Bulletin* available on www.visa.com/cisp
- Take precautions to secure all PEDs in use…or in storage
- To date no Encrypting PIN Pads (EPP) listed



VISA

Visa Security Alert

16 November 2012

Help Protect Cardholder Data From Attacks on PIN Entry Devices

U.S. *| Acquirers, Processors, Merchants, Agents*

To promote the security and integrity of the payment system, Visa is reminding clients, merchants and payment system participants of their responsibility to protect cardholder account and PIN data.

Criminals trying to obtain cardholder account and PIN data at the point of sale (POS) frequently target PIN Entry Devices (PEDs) that are known to be vulnerable. Last year, Visa alerted clients that the VeriFone Everest Plus PED was used in tampering and skimming attacks.

Evidence indicates that these devices were removed from the point of sale and replaced with modified devices designed to capture magnetic stripe card and PIN data, which was then transmitted to criminals wirelessly. Surveillance footage shows that the suspects were able to remove a PED and install a modified device in less than one minute.

Recommended Mitigation Strategies

All VeriFone Everest Plus users are encouraged to upgrade to systems that feature the most up-to-date security

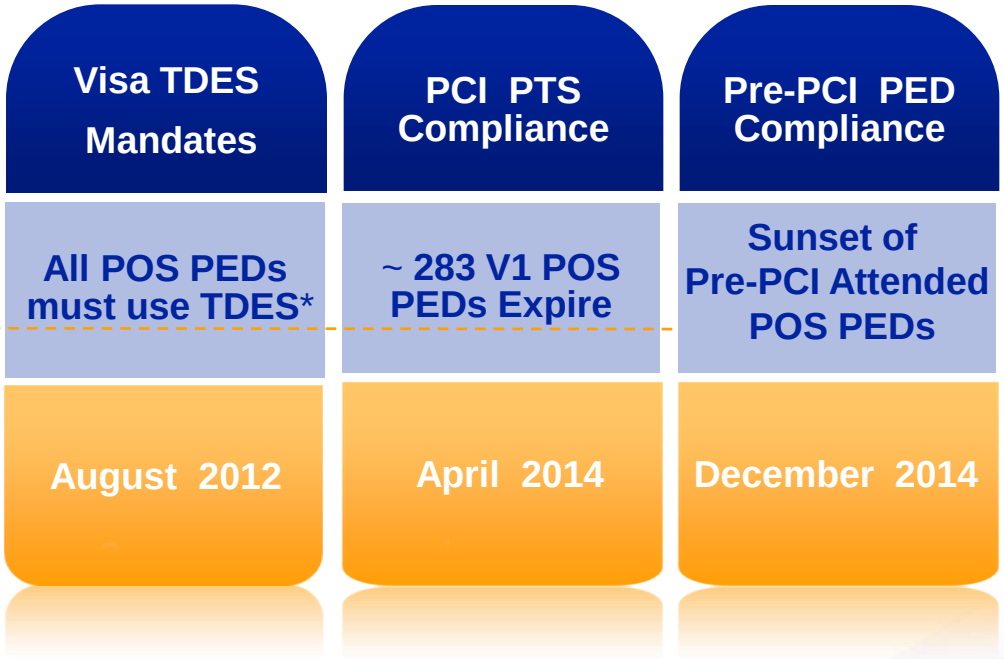
Best Practices to Prevent AFD Skimming

1. Leverage and use vendor controls for AFDs to their fullest extent - Physically secure and alarm AFDs
2. Implement long standing physical security concepts: lighting, robust locks etc.
3. Use terminal authentication systems to detect internal serial numbers and monitor connectivity changes
4. Use terminal asset tracking procedures for devices deployed, stored and shipped

PCI PIN Security Requirements require secure PED management

Future Proof POS Acceptance

- Stay ahead of emerging threats by investing in the most secure equipment
- Align PED retirement / usage mandates with Authentication Roadmap
- Adopt a 'touch once' approach



* TBD for US Automated Fuel Dispensers (AFD)

New PIN Security Compliance Validation Program

Proposed program changes include:

- *Elimination of PIN Security Self-Assessment Questionnaire submission*
- *Introduction of PIN Security Assessors (SA)*
- *Compliant entities listed on Global Registry of Service Providers*
- *Validation cycle every two years*

Program Participants Defined

- PIN Acquiring Third-party VisaNet Processors
- PIN Acquiring Member Service Provider VisaNet Processors
- PIN Acquiring Third-party Servicers (TPS)
- Encryption and Support Organizations (ESO)

Are you on the list?
Global Registry of Service Providers

www.visa.com/splisting

Visa PIN Security Resources

www.visa.com/cisp

PIN Security Program Information:

- Compromised POS PED Bulletins
- PIN Security Alerts & Bulletins
- *Listing of Pre-PCI Approved PEDs*
- *Visa PED Frequently Asked Questions*
- *Visa PIN Security Auditor's Guide*
- *Visa What to do if Compromised*
- Other PIN security related information

pinna@visa.com