Americas Merchant PIN Security Compromise Trends and Best Practices Webinar

February 13, 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.

Agenda

- PIN-Entry Device (PED) Compromise Trends and Security Vulnerabilities
- Review of recent attacks and best practices for prevention
- Review of Visa PED Usage Mandates
  - Review of Visa's PED Retirement Mandates
- Review of PED Usage Best Practices
- An Overview of Visa's US Authentication Announcement
- Q & A

NOTE: This deck will be posted on www.visa.com/cisp

Global Payment Systems Risk Strategy

A multi-layered approach

Build and **enhance** stakeholder trust in
Visa as the most secure way to pay and be paid

PIN Entry Device (PED) Tampering Cases

- **Number of PED tampering cases increasing**
  - Criminals target merchants with certain PED models
    - Attacks on older vulnerable PEDs and newer PED models
    - Wireless models becoming a target
  - Small and large merchants, often multiple stores, targeted
    - Swap out PEDs with altered PEDs
- **Attacks are more sophisticated & technically advanced**
  - Recent attacks involved *VeriFone Everest and Ingenico i3070 PED* models
  - However new PED models are being targeted
- **Evidence of technology being exported globally**

PED Tampering usually involves:

- A second mag stripe reader or connection to existing reader
- Additional circuit board(s)
- Keypad membrane
- Bluetooth device
- Flash memory chip or drive

Americas PED Tampering

North America

- Attacks on chain stores with older POS PEDs
- POS PEDs not well secured
- Criminals travel across country replicating attack
- Perform ATM cash-outs immediately

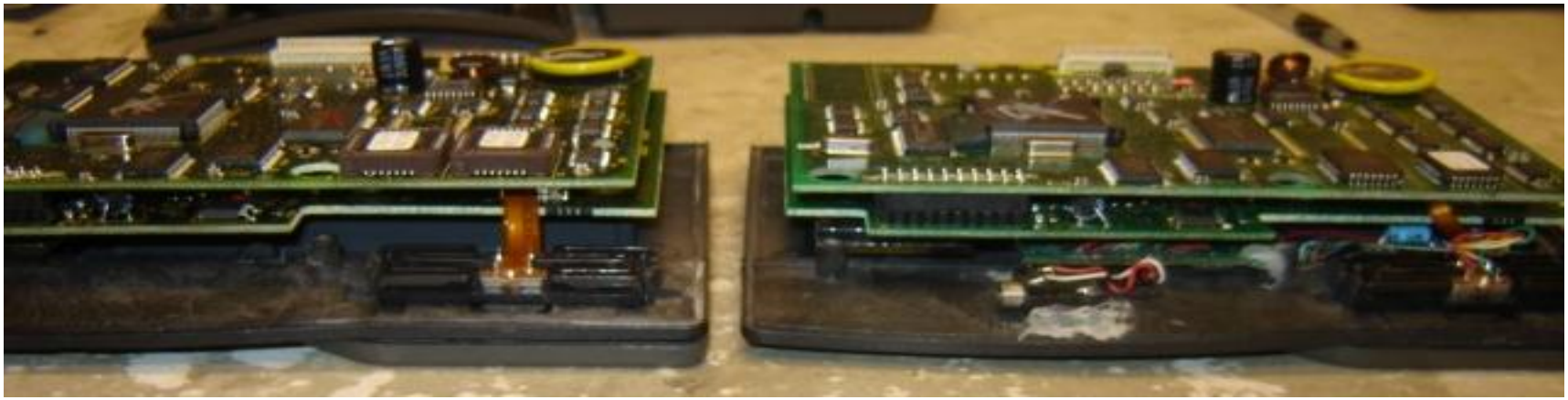
Latin America

- Attacks in Peru, Chile and Colombia
- Highly sophisticated attacks
- PED swaps involved social engineering
- Newer PCI approved PEDs found
- Wireless PEDs targeted, difficult to physically secure

VeriFone Everest

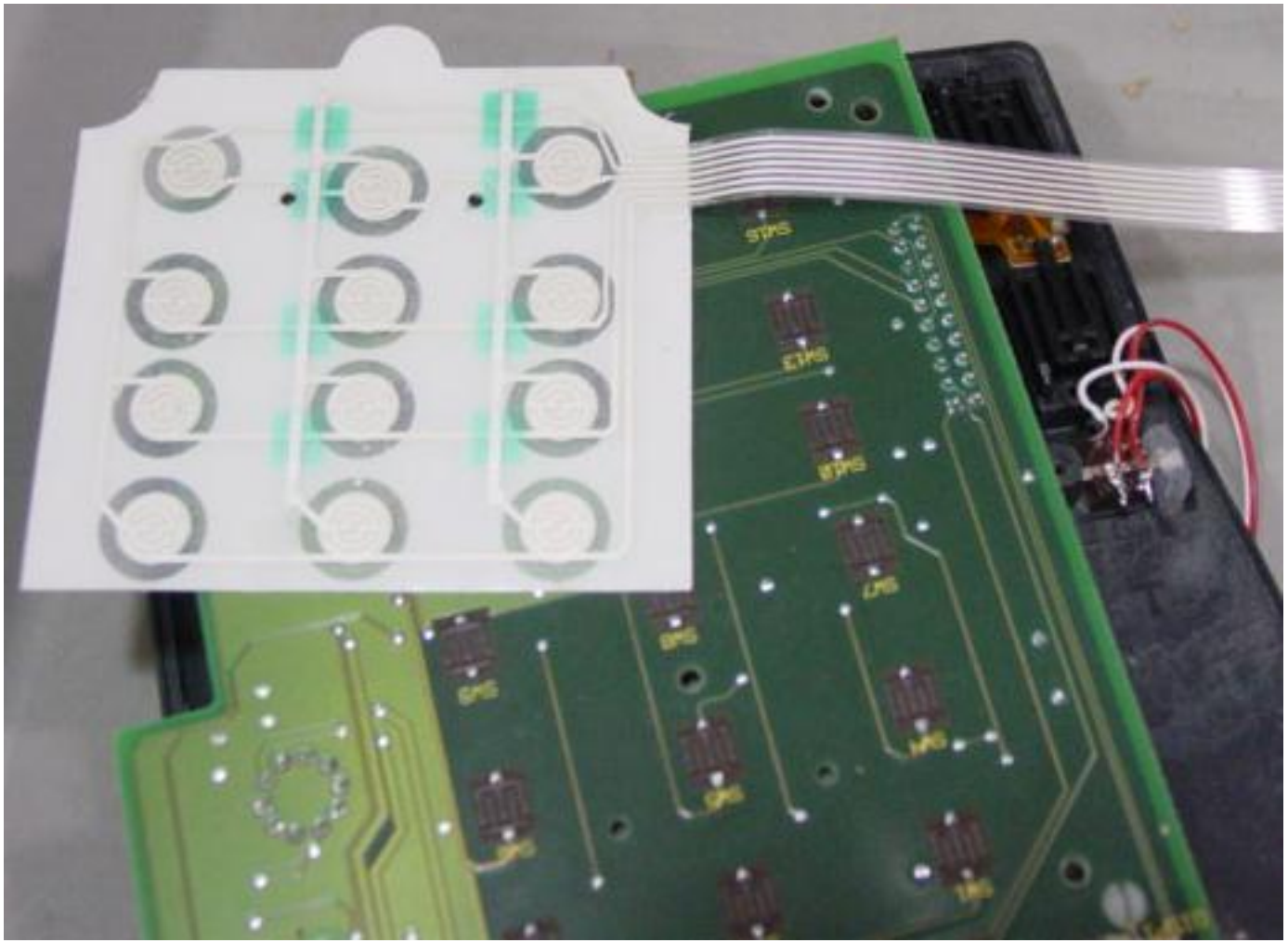
Normal

Tampered



PED Tampering

Membrane keyboard to capture PINs



Preventive Measures for PED Tampering

- Replace vulnerable PEDs as quickly as possible
- Train staff to regularly inspect PEDs visually to identify anything abnormal such as
  - Missing or altered seals or screws
  - Extraneous wiring, holes in the device, or the addition of labels
  - Overlay material used to mask damage from tampering
- Ensure PEDs are physically secured / locked down to counters

Review Visa's Terminal Usage Best Practices:

"Point-of-Sale Terminal Tampering Is a Crime …and You Can Stop It"

www.visa.com/cisp

VISA

Point-of-Sale Terminal Tampering Is a Crime . . . and You Can Stop It

Increasingly, criminals with sophisticated tools are actively targeting vulnerable merchant point-of-sale (POS) terminals to steal payment card data and PINs for counterfeit fraud purposes. That's the bad news! The good news is that all acquirers, merchants, and processors can take appropriate steps to eliminate POS terminal weaknesses and the possibility of POS tampering.

Criminal gangs worldwide are illegally accessing active POS terminals and modifying them by inserting an undetectable

What to do if PED Tampering is Detected

- **Contain and limit the exposure**
  - Remove/unplug suspected PED(s) from your network
  - Secure and safeguard all PEDs
  - For multi-lane locations, track PEDs to a specific lane/register
  - Large merchants should have incident response plans for compromise events
- **Alert all necessary parties**
  - Follow steps in Visa's ***What to do If Compromised*** document on www.visa.com/cisp
  - Notify your sponsoring merchant bank and processor
  - Notify Visa Fraud Control
  - Notify your PED vendor
  - PED Vendors must notify the PCI Security Standards Council
- **Notify Visa Incident Response team** if unable to contact sponsor bank:
  - **U.S.** – (650) 432-2978 or usfraudcontrol@visa.com
  - **Canada** – (416) 860-3090 or CanadaInvestigations@visa.com
  - **Latin America & Caribbean** – (305) 328-1713 or lacfraudinvestigations@visa.com

Securing the Payment System

Visa data security programs drive payment system security

PCI Data Security Standard (PCI DSS)

- Drive PCI DSS compliance to ensure entities protect cardholder data

PCI PIN Security Requirements

- Advance compliance to prevent PIN compromises

PCI PIN Transaction Security (PTS) Testing program

PCI POS PCI EPP

PCI Payment Application Security Standard (PA-DSS)

- Promote development and use of secure payment applications

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

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

Known Compromised Attended POS PEDs

Compromised Non Lab-Evaluated PEDs

Ingenico	VeriFone	Hypercom
• eN-Crypt 2400	• PINpad 101, 201, 2000	• S7S
• C2000 Protégé	• Everest	• S8
	• Everest Plus (-0.X)	

Mandatory sunset date July 2010

Compromised Pre-PCI PEDs

Ingenico	VeriFone
• eN-Crypt 2100	• Everest Plus (-1.X)

Mandatory sunset date Dec. 2014 or earlier!

Compromised PCI PEDs

Ingenico

- i3070MP01
- i3070EP01

Visa has no sunset dates for PCI approved PEDs

Compromised PEDs listed on www.visa.com/cisp

Merchant Best Practices to Prevent Skimming

1. **Implement a terminal authentication system to detect internal serial number or connectivity changes**
2. **Secure terminals / PEDs to counters to prevent removal and secure cable connections**
3. **Inspect and secure PEDs within unattended self checkout lanes**
4. **Use terminal asset tracking procedures for devices deployed, stored and shipped**
5. **Secure stored PEDs and validate inventory against asset records**

- www.pcisecuritystandards.org/documents/skimming_prevention_IS.pdf

Attended POS PED Categories

Non Lab-Evaluated / Non Visa Approved

- PEDs deployed prior to January 2004
- Mandatory Visa sunset date July 2010

Pre-PCI Approved PEDs

- Deployed since January 2004
- Expired on Dec. 2007
- Mandatory Visa sunset date Dec. 2014
- Listed on: www.visa.com/cisp

PCI Approved PEDs

- PEDs deployed since Dec. 2007
- 253 V1 PEDs expire April 2014
- Visa has no sunset date for PCI Approved PEDs
- Listed by PCI SSC

Best Practices for POS PED Acquisitions:

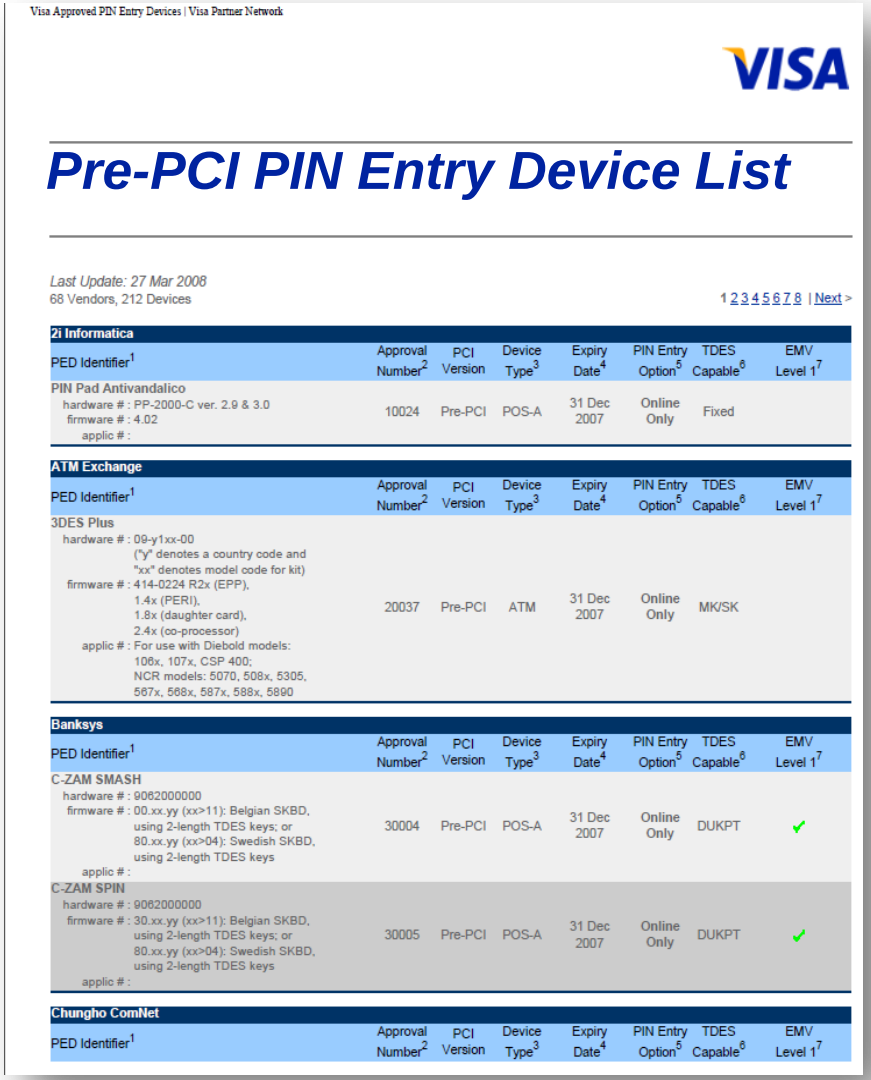
- **Locate PED on PCI PTS website to validate approval status**
- **Keep print screen of PCI PED approval with PO**
- **Purchase the latest version of PCI PEDs when possible – V3**

Pre-PCI PIN Entry Device Listing

Pre-PCI PED Usage Rules

1. **Entire list of devices are expired**
2. **Expired PEDs cannot be purchased or newly deployed**
3. **All attended Pre-PCI POS PEDs must be retired by December 2014**
4. **Entities should plan now to comply with Visa mandatory sunset date**
5. **Pre-PCI PIN Entry Device List**

   www.visa.com/pin



Visa Approved PIN Entry Devices | Visa Partner Network

VISA

Pre-PCI PIN Entry Device List

Last Update: 27 Mar 2008
68 Vendors, 212 Devices

1 2 3 4 5 6 7 8 | Next >

2i Informatica

PED Identifier[1]	Approval Number[2]	PCI Version	Device Type[3]	Expiry Date[4]	PIN Entry Option[5]	TDES Capable[6]	EMV Level 1[7]
PIN Pad Antivandalico hardware # : PP-2000-C ver. 2.9 & 3.0 firmware # : 4.02 applic # :	10024	Pre-PCI	POS-A	31 Dec 2007	Online Only	Fixed	

ATM Exchange

PED Identifier[1]	Approval Number[2]	PCI Version	Device Type[3]	Expiry Date[4]	PIN Entry Option[5]	TDES Capable[6]	EMV Level 1[7]
3DES Plus hardware # : 09-y1xx-00 ("y" denotes a country code and "xx" denotes model code for kit) firmware # : 414-0224 R2x (EPP), 1.4x (PERI), 1.8x (daughter card), 2.4x (co-processor) applic # : For use with Diebold models: 106x, 107x, CSP 400; NCR models: 5070, 508x, 5305, 567x, 568x, 587x, 588x, 5890	20037	Pre-PCI	ATM	31 Dec 2007	Online Only	MK/SK	

Banksys

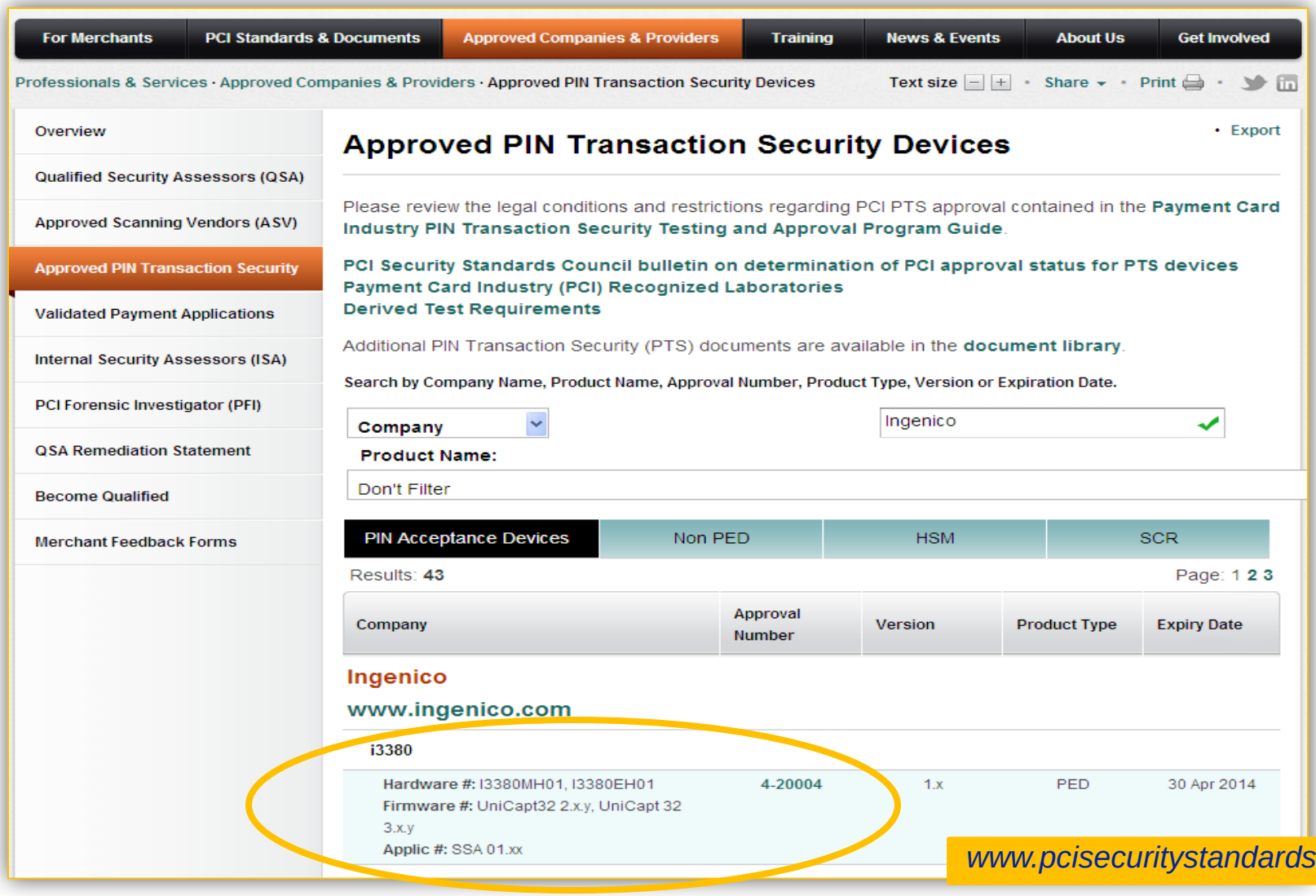
PED Identifier[1]	Approval Number[2]	PCI Version	Device Type[3]	Expiry Date[4]	PIN Entry Option[5]	TDES Capable[6]	EMV Level 1[7]
C-ZAM SMASH hardware # : 9062000000 firmware # : 00.xx.yy (xx>11): Belgian SKBD, using 2-length TDES keys; or 80.xx.yy (xx>04): Swedish SKBD, using 2-length TDES keys applic # :	30004	Pre-PCI	POS-A	31 Dec 2007	Online Only	DUKPT	✔
C-ZAM SPIN hardware # : 9062000000 firmware # : 30.xx.yy (xx>11): Belgian SKBD, using 2-length TDES keys; or 80.xx.yy (xx>04): Swedish SKBD, using 2-length TDES keys applic # :	30005	Pre-PCI	POS-A	31 Dec 2007	Online Only	DUKPT	✔

Chungho ComNet

PED Identifier[1]	Approval Number[2]	PCI Version	Device Type[3]	Expiry Date[4]	PIN Entry Option[5]	TDES Capable[6]	EMV Level 1[7]

PCI PIN Transaction Security Devices

- Always validate Hardware, Firmware and Application prior to purchase



www.pcisecuritystandards.org

POS PED Usage, Planning and Acquisitions

- Always purchase the highest PED version
- Never purchase or deploy expired PEDs
- Plan now for the Pre-PCI PED sunset date
- Beware of ‘bargains’ as sunset date approaches
- Remove attended Pre-PCI POS PEDs no later than December 2014
- For more information review **Visa’s *General PED FAQs*** *www.visa.com/cisp*

PCI Approved PIN Entry Devices
www.pcisecuritystandards.org

PCI PED Version	V1	V2	V3
PED/EPP	283	198	112
PCI PED Expiration	4/2014	4/2017	4/2020

PCI PIN Requirements for Secure PED Usage

PCI SSC released updated ***PCI PIN Security Requirements*** in 2011

- New language added to *PCI PIN Security Requirement* 29
- Physical and logical protections must exist for deployed PEDs
- Precautions may include:
  - PEDs physically mounted or tethered to prevent removal
  - Implementation of a terminal authentication system
- Visa effective date for new PCI PIN Security Requirements: July 2012

PCI PIN Modifications – Summary of Changes

PCI Security Standards Council

Requirement	Section(s)	Modification
25	Main Body Normative Annex B	▪ Clarified that no other person (not similarly entrusted with that component) can observe or otherwise obtain the component. ▪ Specified that key custodians sufficient to form the necessary threshold to create a key must not directly report to the same individual.
	Normative Annex A	Increased minimum pass phrase from six to eight characters for Certification and Registration Authority relevant equipment.
	Normative Annex A	Added biometrics as an associated usage authentication mechanism for security tokens
26	N/A	N/A
27	N/A	N/A
28	N/A	N/A
29	Main Body Normative Annex B	Specified that precautions must be taken to minimize the threat of compromise of PIN-processing equipment once deployed.
	Normative Annex B	Specified that secure areas must be established for the inventory of PEDs that have not had keys injected.
30	N/A	N/A

Visa's U.S. Chip Announcement

August 9, 2011

Consider Visa's Chip roadmap as you invest in your next terminal upgrades

1	**Technology Innovation Program**	Starting October 2012, Visa will eliminate the need for eligible merchants to annually validate compliance with PCI DSS for any year in which > 75% of transactions originate from chip-enabled terminals
2	**Develop Chip Processing Infrastructure**	By April 2013 Visa will require processors to support acceptance of EMV chip transactions
3	**Establish Liability Shift**	By October 2015* acquirers/merchants who do not support dynamic data (chip) may be liable for counterfeit fraud

Laying the Groundwork for Dynamic Authentication in the U.S.

* 2017 for Automated Fuel Dispensers

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

Visa TDES Mandates	PCI PTS Compliance	Pre-PCI PED Compliance	CHIP Liability Shift - POS	CHIP Liability Shift - AFD
All POS PEDs must use TDES*	~ 150 V1 POS PEDs Expire	Sunset of Pre-PCI Attended POS PEDs	Deployed Chip devices limits liability	Deployed Chip devices limits liability
August 2012	April 2014	December 2014	October 2015	October 2017

* TBD for US Automated Fuel Dispensers (AFD)

Secure PED Acquisition, Usage and Planning

Acquisitions

- Never purchase expired PEDs
- Always purchase PCI Approved Version 3 PEDs
- Purchase PEDs that are EMV capable

Usage

- Secure PEDs while in stores
- Use a terminal authentication system
- Replace vulnerable PEDs
- Track PED Inventories

Planning

- Retire Pre-PCI Attended POS PEDs by December 2014

Americas Visa PIN Security Trainings

2013 Key Management Training Schedule:

- **PIN Security and Key Management for Plus Agents**
  - February 19, Scottsdale, AZ (English)
- **Key Management & PIN Security Compliance Validation**
  - March 25 – 27, Sao Paulo, Brazil (Portuguese)
  - April 23 - 25, Ashburn, VA (English)
- **PIN Security and Key Management**
  - June 25, Toronto, Canada (English)
  - September 10, Ashburn, VA (English)

For more information go to www.visa.com/cisp

- Trainings are accredited for Continuing Professional Education
- Custom in-house training sessions available
- Contact: VisaBusinessSchool@visa.com

For More Visa PIN Security Information

www.visa.com/cisp

- Compromised POS PED Bulletins
- *Listing of Pre-PCI Approved PEDs*
- *PIN Compliance Validation Framework*
- *Visa PED Frequently Asked Questions*
- *Visa PIN Security Tools and Best Practices for Merchants*
- *Visa PIN Security Program: Auditor's Guide*
- *Visa What to do if Compromised*
- Other PIN security related Bulletins and information
- Global list of ESOs - www.visa.com/merchants/risk_management

Contact: pinusa@visa.com

PCI SSC PIN and PTS Resources

PCI Security Standards Council

www.pcisecuritystandards.org

- New *PCI PIN Security Requirements V1 Sept 2011*
  - *Visa Effective date July 2012*
- PCI PTS Approved PIN Entry Device List
  - Hundreds of Vendors
  - Over 500 PEDs….but try to purchase V3 PEDs only