



PIN Security and Automated Fuel Dispensers

Payment System Risk



Payment System Risk Data Security Webinars Overview



Encourage greater adoption of and adherence to *Payment Card Industry Data Security Standard* (“PCI DSS”) and *PCI PIN Security Requirements*

Promote security awareness

Use frontline information

Create transparency and clarity around PCI rules, roles and responsibilities

Five-Part Security Strategy



Secure the Payment Environment

Monitor, Identify and Prevent Fraud

Manage the Impact of Fraud

Maintain Trust in Visa Payments

Create an Environment of Partnership

Agenda



- Overview of current security threats at AFDs
- Visa's PIN Security Program
- PCI PED testing and Automated Fuel Dispensers ("AFD")
- Track data elimination
- Payment Application Best Practices



Investigative Findings



Increase in reported skimming activity involving MCC 5542

Activity concentrated activity in Southern California and Florida

Specific AFD manufacturers and models targeted

Organized groups target locations: goal is track and PIN data

Documented cases with law enforcement

- Federal: Secret Service
- State: Florida Department of Agriculture and Consumer Services
- Local: West Palm Beach PD, Anaheim PD, Las Vegas Metro PD

Typical Modus Operandi



High volume stations targeted

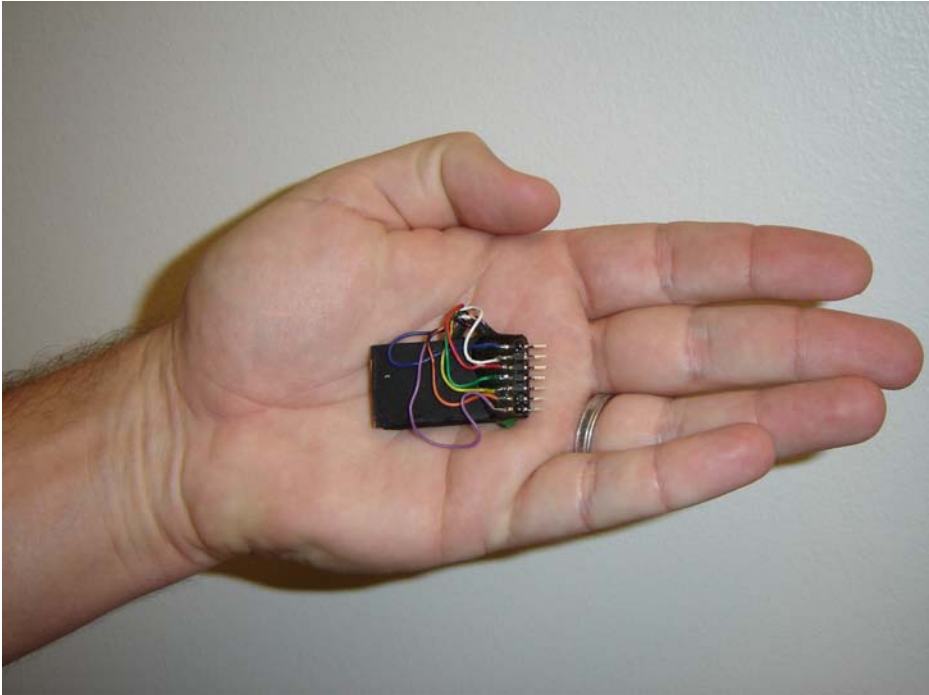
AFD located away from cashier

Access via front panel with shared 'brass key'

Suspects impersonate pump service technicians

Reader device attached to card reader and PIN pad

Typical devices



Typical Devices



Typical Devices



Visa Investigative Initiatives



Assisting issuers to identify AFD skimming

Identifying and obtaining at risk accounts for CAMS distribution

Assisting law enforcement with cases and fraud losses

Building industry awareness through meetings and publications

Visa Business Review August 2006 ref # 060801

Visa Data Security Fraud Alert September 2006 ref # 092906

Visa Security Alert for Petroleum Retailers November 2006

Visa Alerts Members about Payment Applications that Store Prohibited Data VBR October 2007 Ref#071023

To ensure the safety and soundness of electronic payments to support their continued growth

Visa's PIN Security Program



Established in 1995

Worldwide in scope

Designed to protect cardholder PINs during message processing

Requires:

- Compliant equipment for PIN entry
- Specified cryptography to protect PIN during transmission
- Documentation and methods that ensure key secrecy

Failure to comply can result in financial losses and / or other sanctions

Visa PIN Security Program



Visa PIN Security program based on the *Payment Card Industry (PCI) PIN Security Requirements*

Current PCI PIN Security participants:

- Visa
- MasterCard

Compliance required by Visa, Plus and Interlink Operating Regulations

PCI Security Standards Council adopting PCI PED Testing program (all five card brands)



Visa PIN Security Program



Program specifies acceptable cryptography and mandates for usage

- Triple DES

Program specifies acceptable equipment and mandates for usage

- PIN Entry Devices (“PED”)
- Hardware Security Modules (“HSM”)

Program specifies compliant processes

- Dual control
- Split knowledge key management

Program specifies acceptable administrative processes

- Equipment management
- Cryptographic and key management processes

Visa TDES Mandates – US Region

Overview



TDES Usage

International Standards Organization (“**ISO**”) and American National Standard (“**ANSI**”) online and off-line PIN security standards

- **Single DES** has been fully retired by ISO and ANSI

Business Objectives

- Security of payment system
- PIN protection / maintain consumer confidence

Visa Endpoint Mandate:

Effective 12/31/2007

All US VisaNet endpoint issuer Working Keys (“IWKs”) and Acquirer Working Keys (“AWKs”) must use TDES



Hardware	Usage
<p><i>Effective 1/1/2004</i></p> <p>-All newly deployed <i>attended</i> POS PED models (i.e., newly purchased devices from original equipment manufacturer, not previously acquired devices being installed for first time) must be evaluated by Visa-recognized laboratory, and approved by Visa, and must support TDES</p> <p><i>End date 7/1/2010</i></p> <p>-All <i>attended</i> POS PEDs must support TDES and be either pre-PCI or PCI approved</p>	<p><i>Effective 7/1/2010</i></p> <p>-All transactions originating at attended and unattended POS PEDs must be encrypting PINs using TDES from the point of transaction to the issuer (end-to-end)</p>

PED-Testing Program



Acquirers and merchants relied on vendor claims of PED compliance

- Some PEDs proved non-compliant

Independent Labs validate PED compliance

- Visa only (Pre-PCI) PED testing program initiated in 2002, aligned in 2004
- Benefits all stakeholders

Most pre-PCI PEDs removed from list on 12/31/2007

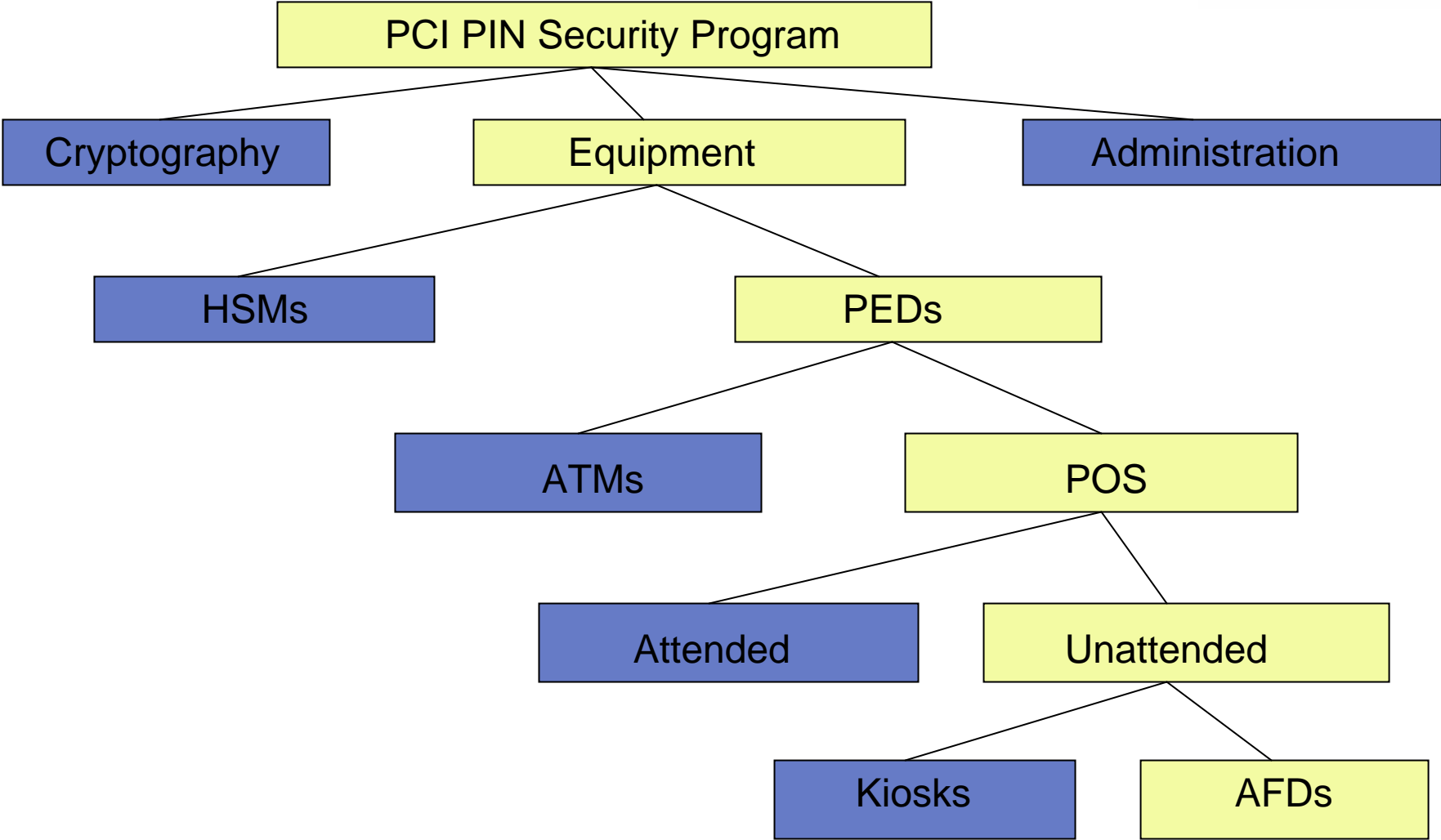
- Pre-PCI PEDs can not be purchased after 12/31/2007
 - Pre-PCI PEDs may continue to be used
 - To remain on list vendors must resubmit
- For more information go to www.visa.com/pin

- Review *General FAQ*
- *PCI PED Testing and Approval Program Guide*

Approved PIN Entry Devices www.visa.com/pin

	<u>Pre-PCI</u>	<u>PCI</u>
Vendors	71	58
POS	155	103
EPP	47	39
ATM	1	0
AFD	2	1

Where Automated Fuel Dispensers Fit



New Classification of POS PED



PCI PED Testing Program participants recognize new **unattended** POS PED category (“AFDs” / Kiosks)

Effective 10/1/2007 - All newly deployed unattended POS PEDs must contain an EPP that has passed testing by an approved lab and is approved by Visa

- Similar to ATM mandate effective 10/1/2005 that all newly deployed ATMs must contain a EPP that has passed testing by an approved lab and approved by Visa

Overall unattended POS PED test requirements in development (not just the EPP)

AFD vendors informed of new PED classification and developing solutions for lab evaluation and approval

New Classification of POS PED cont.



Merchants should contact AFD vendors for timeframes / delivery of approved PEDs

Merchants must have plans in place to integrate new EPPs and begin deployments when available from Vendors

Merchants should evaluate TDES usage at the time of the EPP deployments – multiple key registers (SDES & TDES)

US AFD acquirers have been granted an extension to deploy PCI approved unattended POS PEDs / EPPs until January 1, 2009

- There is no waiver of liability

Extension does not cover the face-to-face POS PEDs at oil merchants – only the AFD

Approved PED Deployment Mandates



Attended POS PEDs - 1/1/2004

- Newly purchased from Original Equipment Manufacturer
- As of 7/1/2010 **all** attended POS PEDs must be either pre-PCI or PCI approved – date aligns with TDES usage mandate

Unattended POS PEDs - 10/1/2007

- Newly deployed kiosks must have a PCI-approved EPP
- Newly deployed AFDs (not in US) must have a PCI-approved EPP
- Overall unattended POS PED requirements in development

Unattended POS PEDs (US AFDs Only) - 1/1/2009

- Newly deployed AFDs must have a PCI-approved EPP

ALL POS PEDS MUST BE USING TDES by 7/1/2010 GLOBALLY!

- Single-DES DUKPT not acceptable

PED Acquisitions



Transition to PCI approved PEDs – PCI approved PEDs are tested under more rigorous requirements

- Most Pre-PCI PEDs will expire and be removed from the approved list December 31, 2007
- Pre-PCI PEDs can not be purchased if they are not on the list at the time of purchase

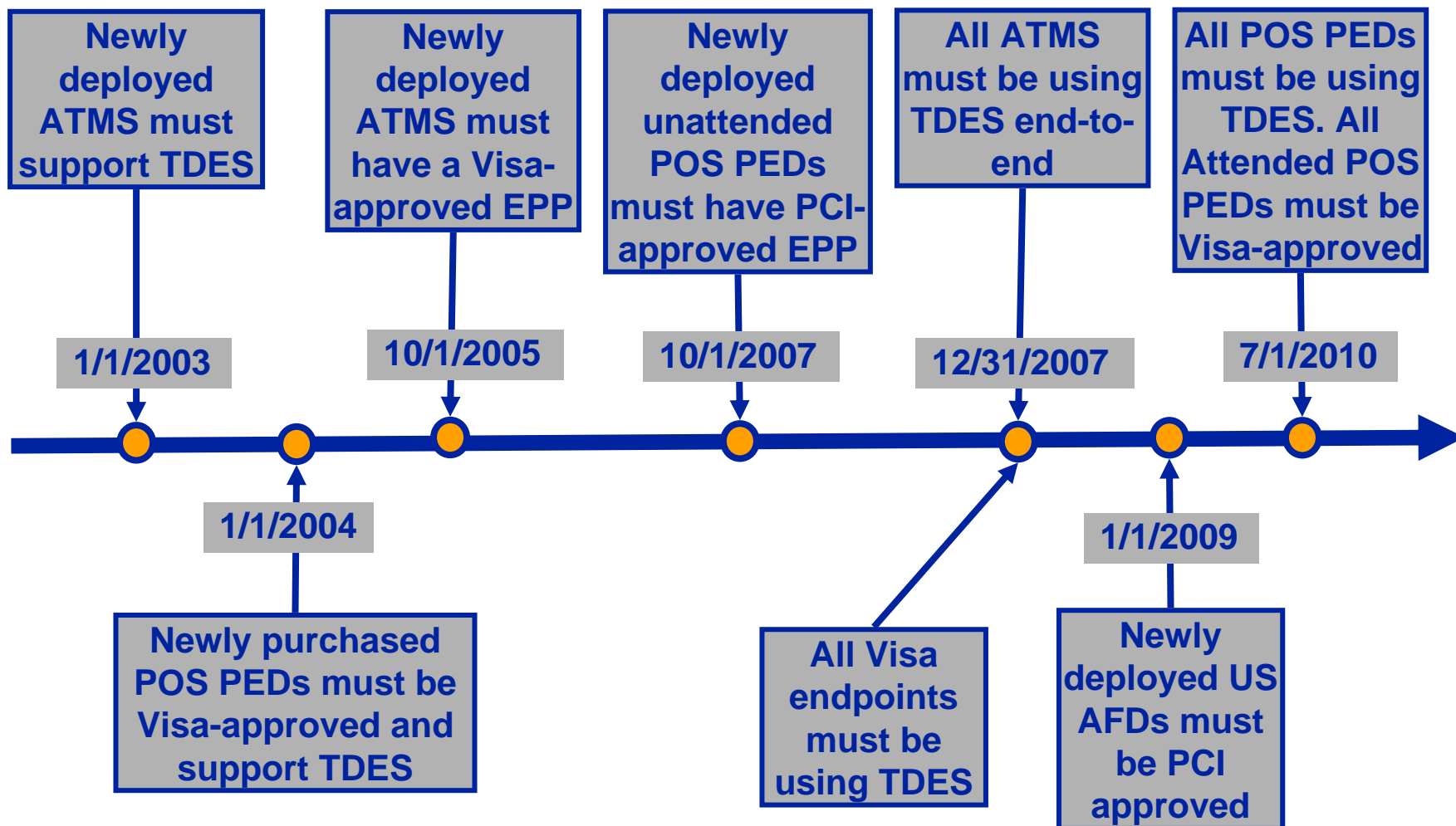
Ensure that any newly purchased PEDs are PCI-approved and listed on the Approved Device List on and after January 1, 2008

Include language in purchase agreement that binds manufacturer to supply only PCI approved devices

- Ensure that both the device and the software / firmware are approved

Attach the relevant section of the PCI Approved Device List to the purchase contract

Visa U.S.A. TDES and PED Testing Timeline



Sensitive Data Elimination



PCI DSS and PCI PIN Security Requirements prohibit the storage of sensitive cardholder-specific data

- PIN block
- Track 1 data
- Track 2 data
- Some Visa transactions require track data and PIN blocks in non-original messages
 - May need to be stored



Track Data Elimination



- Interlink and other US debit networks require that full track and PIN data be provided in several non-original messages:
 - Reversals
 - Pre-authorization Completions
- Visa developed an aligned solution with the other networks
- **Effective October 2007**, all Visa issuer processors must be able to receive non-originals without Track and PIN data
 - Acquirers may optionally begin to send non-originals without track and PIN data
- **Effective April 2008**, all Visa acquirer processors must not send track and PIN data in non-originals
 - Merchant level compliance date TBD
- Please see the International Business Enhancements Technical Letter for the October 2007 release, section 1.6 on www.visaonline.com

Upcoming Visa Security Workshops



Three Day Visa PIN Security Auditor's Workshop

May 13 -15, 2008 – Chicago, IL

One Day Visa Key Management Workshops

February 20, 2008 – New Orleans, LA with ATMIA

June 5 and October 9, 2008 – Foster City, CA

- To receive information on workshops contact:
pinusa@visa.com

PCI DSS Training for Merchants and Acquirers

June 3 - 4, 2008 – Foster City, CA

- To receive information on workshops contact:
cisp@visa.com

Payment Application Mandates



Visa USA is aggressively driving the adoption of secure payment applications in the marketplace

Phase	Compliance Mandate	Effective Date
I.	Newly boarded merchants must not use known vulnerable payment application and VNP and agents must not certify known vulnerable payment applications	1/1/08
II.	VNP and agents must certify only PABP-compliant payment applications to their platforms	7/1/08
III.	Newly boarded Level 3 and 4 merchants must be PCI DSS compliant or utilize PABP-compliant payment applications*	10/1/08
IV.	VNP and agents must decertify all known vulnerable payment applications**	10/1/09
V.	Members must ensure their merchants, VNP and agents use PABP-compliant payment applications	7/1/10***

* In-house use only developed applications & stand-alone POS terminals are not applicable

** VisaNet Processors and agents must decertify vulnerable payment applications within 12 months of identification

***Date is aligned with TDES mandate for all POS PEDs to support TDES and be Visa-Approved/Lab-Evaluated

PCI Security Standards Council (PCI SSC)

- Data Security Standard
- Security Audit Procedures
- Self-Assessment Questionnaire
- Security Scanning Procedures
- Qualified Security Assessor List
- Approved Scan Vendor List
- Glossary of Terms

www.pcisecuritystandards.org

Visa CISP

- Archive of Data Security Alerts, bulletins and webinars
- What To Do If Compromised guide
- Qualified CISP Incident Response Assessor List
- List of CISP-Compliant Service Providers
- Payment Application Best Practices
- List of Validated Payment Applications

www.visa.com/cisp

www.visa.com/pabp

For More Information



[**www.visa.com/pin**](http://www.visa.com/pin)

PCI PIN Security Requirements & Normative Annex A

PCI POS PIN-Entry Device Security Requirements

PCI EPP PIN-Entry Device Security Requirements

PCI PIN Entry Device Testing and Approval Program Guide

Visa PIN Security Tools and Best Practices for Merchants

Visa PIN Security Program: Auditor's Guide

PCI Key Injection Facility Security Requirements - Draft

Frequently Asked Questions