



PCI DSS

Andrew Mulvenna

AIS Technical Manager

Visa Europe

The PCI Security Standards Council

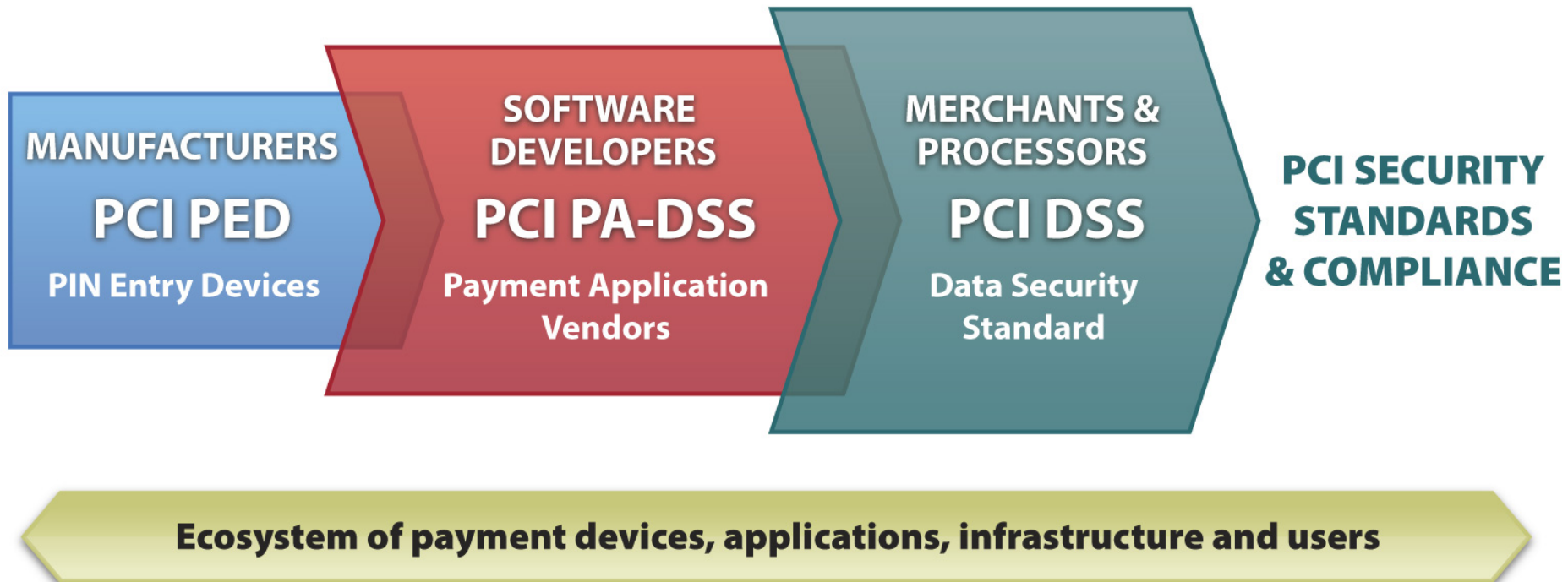


PCI SSC - Standards



PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



PCI DSS: Myths and Facts

Myths

- PCI DSS compliant entities have been breached
- PCI DSS does not address sniffer* attacks
- Visa does not support encryption
- Encryption of data transmission could have prevented recent compromises



Facts

- As of today, no compromised entity has been found to be compliant at the time of the breach
- PCI DSS should prevent and detect unauthorised network access and installation of sniffers
- Visa does support encryption for both online and batch files
- Encryption does provide protection but data needs to be encrypted throughout the processing chain



PCI DSS continues to serve as a robust foundation to protect cardholder data in a static data environment

*Sniffers are used by hackers to monitor and capture data in transit over an internal network

Too much emphasis on PCI DSS validation finish line rather than security and compliance leaves compromise risk

- PCI DSS controls, when implemented properly, would prevent network intrusions
 - If the network is compromised, impact should be mitigated via timely detection
- In all compromise cases, forensic investigations have found significant gaps in the compromised entity's PCI DSS controls to be major contributors to the breach
- Validating compliance is a snapshot, point-in-time review of a business' systems, and is limited in scope to a sample of systems
 - Entities must not rely solely on a Qualified Security Assessors to determine their compliance
 - PCI DSS can no more account for every eventuality than a financial audit can review all the financial transactions of a company
- Maintaining good security requires an ongoing commitment
 - PCI DSS compliance is a 24 hour a day, 7 day a week, 365 day a year job
 - Businesses must build ongoing compliance monitoring into their internal auditing processes

Compromise Trends – Global

»» As PCI DSS compliance rates rise, new compromise trends emerge

Compliance Milestone

- PCI DSS compliance is adopted by acquiring participants in the U.S.
- Merchants and service providers reduce historical storage of cardholder data
- PCI DSS compliance improves among large merchants
- E-commerce and payment channel websites better secured

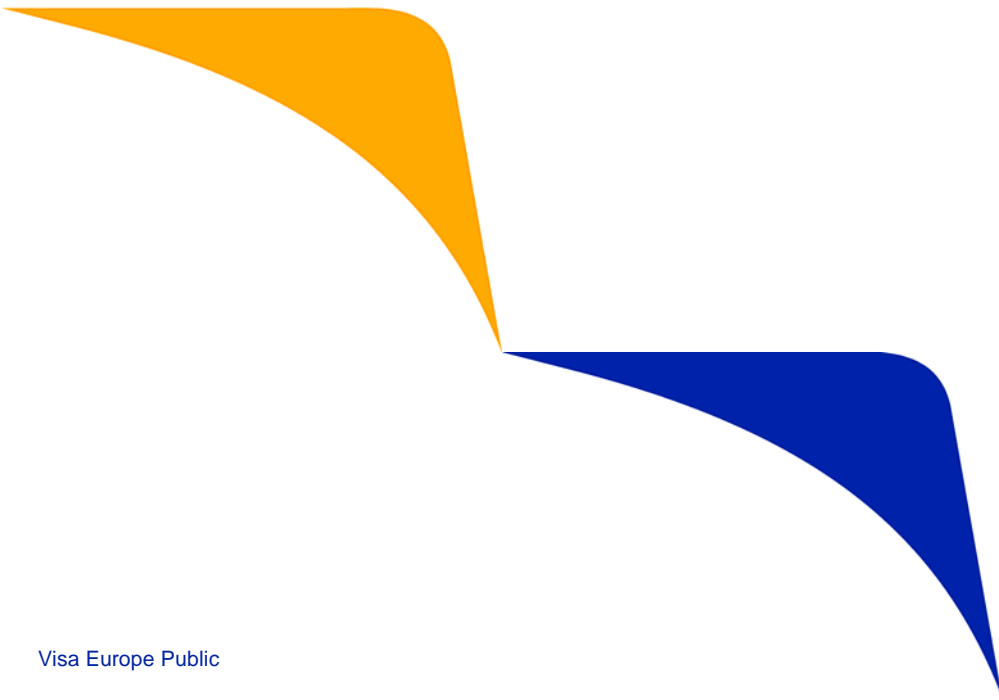


Compromise Trend

- Issuers and processors increasingly targeted; non-U.S. compromises increasing rapidly
- Data criminals seek capture of cardholder data in transit through sniffer attacks
- Compromises of small and medium size merchants increase
- SQL injection attacks on non-payment sites to gain access to payment environment



The evolution of fraud



The evolution of bank card fraud



	1980	1990	2000	Today
Fraudster	Individuals	Teams	Local crime rings	International crime rings
Target	Consumers	Small retailers	Larger retailers	Banks Processors
Leading fraud types	Lost/stolen Intercepted	Domestic counterfeiting/ skimming	Identity theft Phishing Rudimentary data compromise	Cross-border data compromise CNP fraud ATM fraud
Type of cards targeted	T&E cards	Premium credit cards	Mass market credit cards	All types of credit cards Debit cards Prepaid cards
Necessary resources	Opportunism	Rudimentary knowledge	Technical knowhow	Audacity Technical expertise Insider information Global connections

A growing threat¹



285 Million Records compromised in 2008

- More than the previous four years combined
- 91% of records compromised by organized criminal groups
- 99.6% of records compromised from servers and applications
- 69% were discovered by a 3rd party
- 67% were aided by significant errors
- 32% implicated business partners (e.g. service providers)

¹ Source: Verizon 2009

Breaches – some truths¹



66% involved data the victims did not know was on the system

83% of attacks were not highly difficult

87% were considered avoidable through reasonable controls

90% of records were compromised as a result of targeted attacks

- The victim was chosen and then a vulnerability to get access was identified
- This figure was 14% in the 4 previous years

¹ Source: Verizon 2008



Visa Europe Compliance Framework

Visa Europe mandates



- Acquirers must register all third parties with Visa Europe and ensure they are compliant
- Focus on payment application standards
 - All merchants to upgrade to applications that do not store sensitive data by July 2010
 - Merchants should only use payment applications that have are compliant with PA-DSS by Dec 2012
- Large non e-commerce merchants should already be compliant
 - The ones that are not have presented an action plan to Visa Europe and this has been accepted
 - All e-commerce merchants must either validate compliance, or use compliant service providers by October 2009



Risk Based Approach

PCI DSS Risk-Prioritised Phases



Phase	PCI DSS Objective (defined by PCI SSC)
1	Remove Sensitive Authentication Data and Limit Data Retention
2	Protect the Perimeter, Internal, and Wireless Networks
3	Secure Applications
4	Protect Through Monitoring and Access Control
5	Render Cardholder Data Unreadable
6	Achieve Final Compliance and Maintenance of PCI DSS

Reduce your risk early - prioritise



- Identify payment transaction flow
- Remove sensitive data
- Ensure other links in chain are secure
- Protect perimeter defences
- Secure individual applications
- Passwords, access controls and System monitoring
- Render any remaining card data unreadable
- Policies





Payment Applications

Payment Application Vulnerabilities



Numerous payment applications have played a role in data compromises

- Visa responded by developing PABP – now PA-DSS

The top 5 payment application vulnerabilities include:

- Full track data and/or encrypted PIN block retention
- Default accounts and passwords
- Insecure remote access by software vendors and their resellers
- Compatibility issues with anti-virus and encryption
- SQL injection

PA-DSS Applicability



Type of Payment Application *	Does PA-DSS Apply?
“Off-the-shelf” standard payment applications without much customization	YES
Software developed in modules	YES, applies to any module with payment functions
Software for only one, typically large, customer, developed to customer’s specifications	NO, application is covered as part of customer’s PCI DSS review BUT – can use PA-DSS methodology
Software developed by merchant or service provider, and used only in-house	NO, application is covered as part of merchant’s or service provider’s PCI DSS review BUT – can use PA-DSS methodology
Supporting systems, for example, operating systems, databases, back-office systems, firewalls, routers, etc.	NO, these are NOT payment applications

*Payment applications are those that store, process, or transmit cardholder data as part of authorization or settlement.

PCI DSS Compliance is still the Payment Card Industry's 'default' position to secure cardholder data.

In parallel Visa Europe is developing a risk reduction framework to :

- Assess alternative and complementary solutions to PCI DSS
- Engage Stakeholders and provide guidance on solutions
- Identify Risks and Issues with solutions

Innovations that complement PCI DSS

- Assess alternative and complementary solutions to PCI DSS
 - Identify new approaches
 - End-to-end (or point-to-point) encryption
 - Tokenization
 - Evaluate approaches
 - Mitigate Risk rather than achieve compliance

Where to find information



Visit the Visa Europe website at:

<http://www.visaeurope.com/ais>

Contact Visa Europe

Email: datasecuritystandards@visa.com

Visit the PCI SSC website at:

<http://www.pcisecuritystandards.org>



Thank you