PCI DSS

Payment Card Industry Data Security Standard Overview

10-July-2009

Michael De Iulio

Quản lý sự phát triển.

WORLDSOFT

PCI DSS Overview

Topics, Terms, Notes

- **PCI** – Payment Card Industry
- **QSA** - Qualified Security Assessors
  - PA-QSA - Payment Application Qualified Security Assessors
- **ASV** - Approved Scanning Vendors
- **PCI SSC** – PCI Security Standards Council
- **Acquirer** – Acquiring Bank or Acquiring Financial Institution. Entity that initiates and maintains relationships with merchants for the acceptance of payment cards

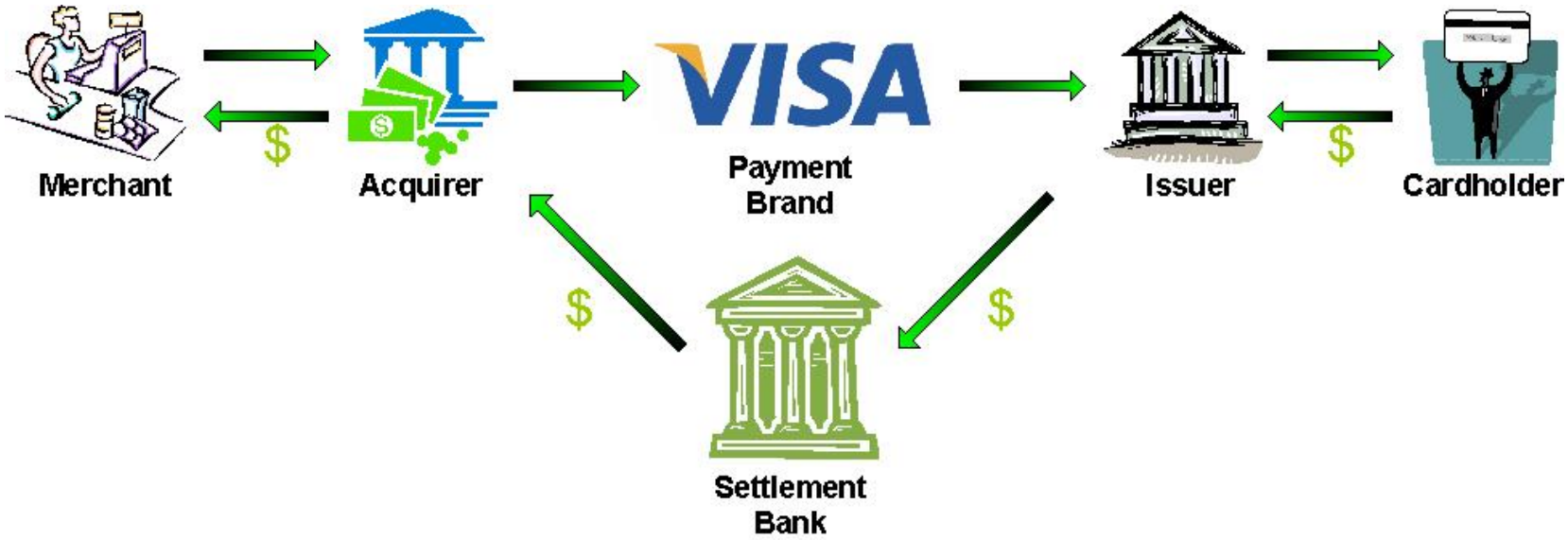
Topics, Terms, Notes

- **ROC** – Report On Compliance
- **SAQ** – Self-Assessment Questionnaire

Topics, Terms, Notes

- x

Payment Card Purchase Process



- **Acquirer** – Merchant's Bank
- **Issuer** – Issues payment card to cardholder

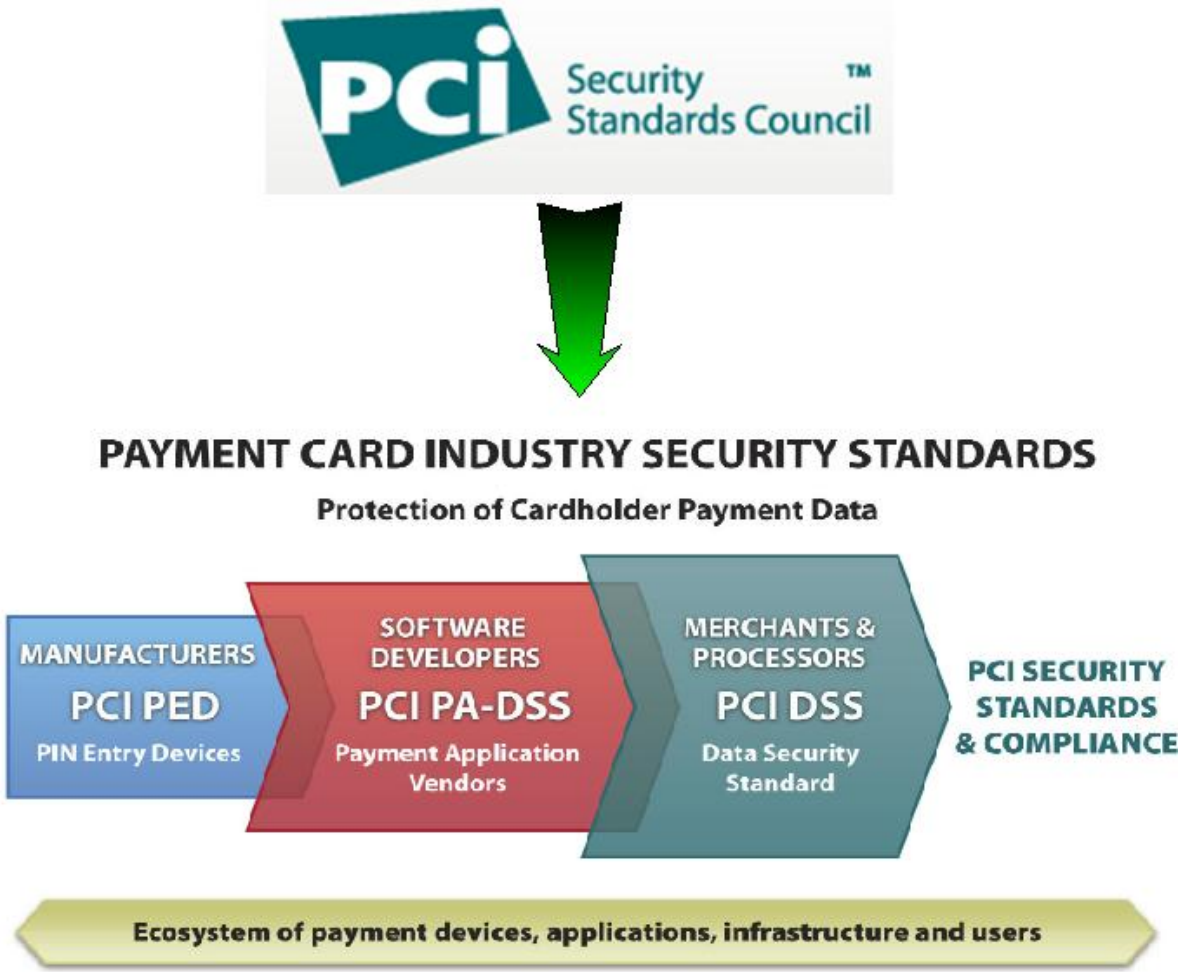
Threats

- 234 Million records with sensitive information have been breached since Jan 2005 according to Privacy Rights Clearinghouse.org

PCI SSC Founders

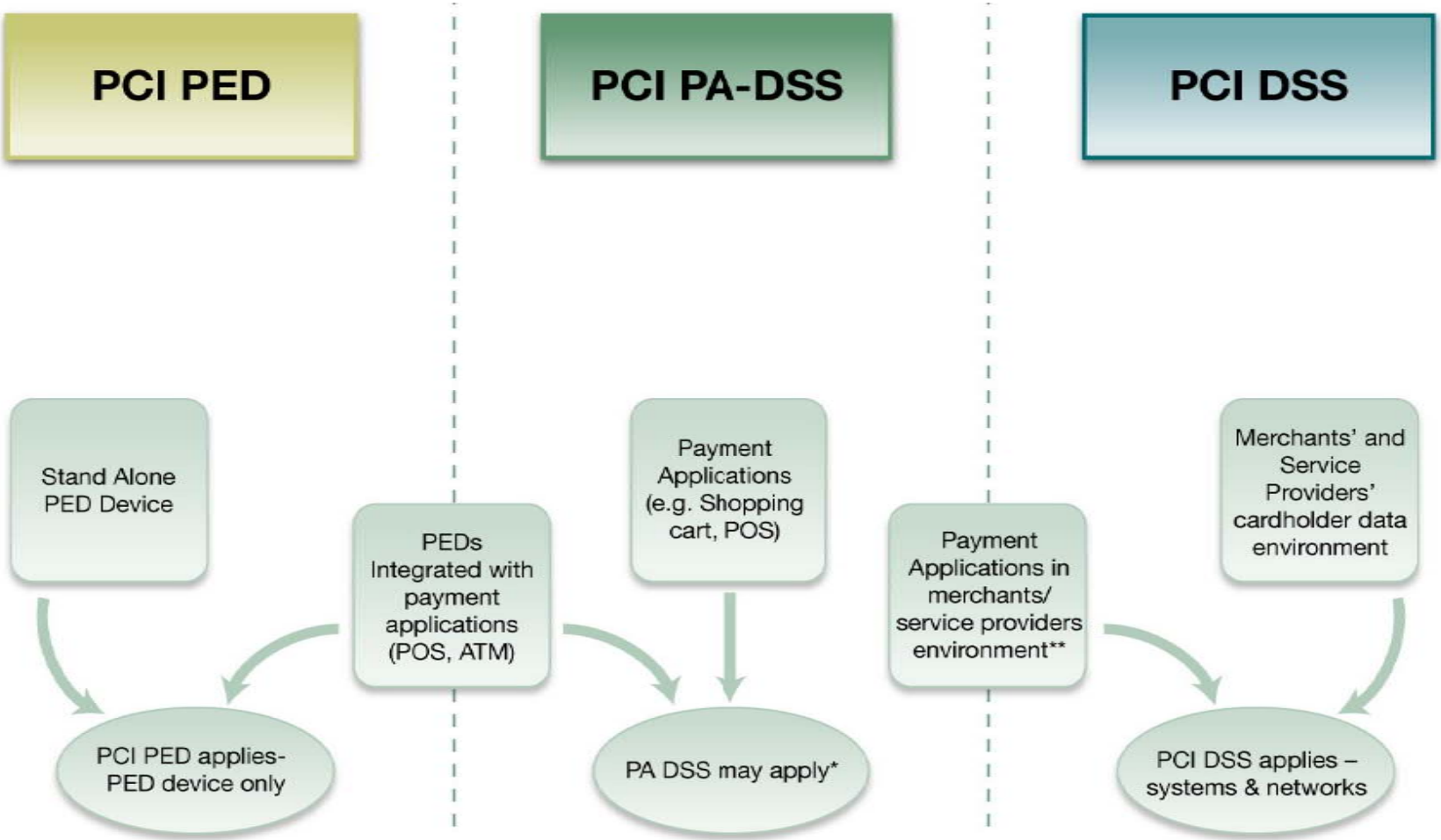
- PCI SSC
  - Security Standards Council
  - Sets security standards
  - Founders
    - Visa, MC, AMEX, Discover, JCB
  - Each brand has own compliance program
    More info in Links
  - Participants:
    - banks, processors, developers, POS vendors

PCI Security Standards



- Reference https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf

Relationship Between Standards



PCI Security Standards

- PCI PED
  - Applies to manufacturers who specify and implement device characteristics and management for personal identification number (PIN) entry terminals used for payment card financial transactions

PIN Entry Device Security Requirements – Validated by PED Laboratory
Device Characteristics
Physical Security Characteristics (to prevent the device from being stolen from its location)
Logical Security Characteristics (to provide functional capabilities that ensure the device is working appropriately)
Device Management
Device Management during manufacturing
Device Management between manufacturer and initial cryptographic key loading
Considers how the PED is produced, controlled, transported, stored and used throughout its lifecycle (to prevent unauthorized modifications to its physical or logical security characteristics)

PCI Security Standards

- PCI PA-DSS
  - For software developers and integrators of applications that store, process or transmit cardholder data as part of authorization or settlement.

Payment Application DSS Requirements – Validated by PA-QSA Assessment	
1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CIV2, CW2) or PIN block data	8. Facilitate secure network implementation
2. Provide secure password features	9. Do not store cardholder data on a server connected to the Internet
3. Protect stored cardholder data	10. Facilitate secure remote software updates
4. Log application activity	11. Facilitate secure remote access to application
5. Develop secure applications	12. Encrypt sensitive traffic over public networks
6. Protect wireless transmissions	13. Encrypt all non-console administrative access
7. Test applications to address vulnerabilities	14. Maintain instructional documentation and training programs for customers, resellers and integrators

PCI Security Standards

- PCI PA-DSS
  - Global data security standard requirements for merchants and service providers that store, process, or transmit cardholder data.
  - Business of any size must adhere to in order to accept payment cards.
  - Each brand has own compliance program See “Links” for more information

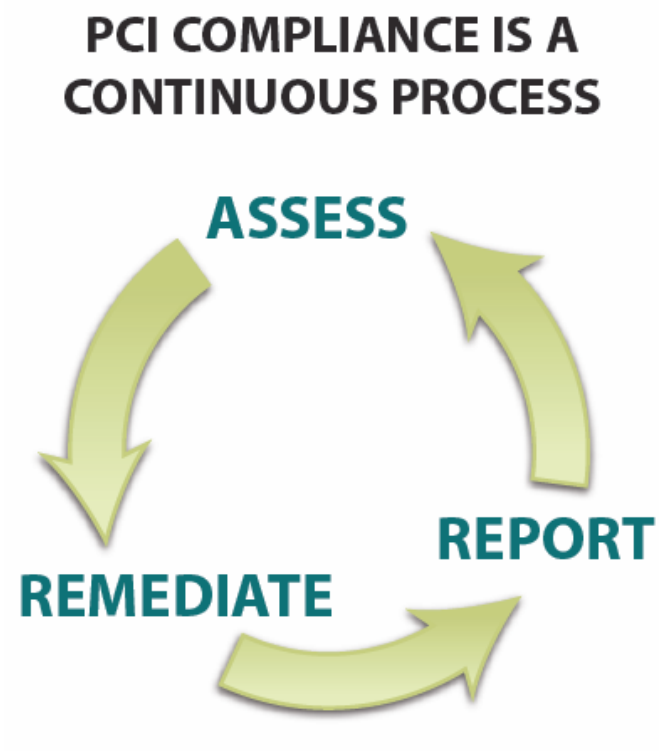
PCI Security Standards

- PCI PA-DSS (12 Requirements)

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

PCI DSS Compliance

- **Assess** - Process of inventorying of IT assets and business processes, and analyzing them for vulnerabilities that could expose cardholder data.
- **Remediate** - Fixing vulnerabilities.
- **Report** - Compilation of records required by PCI DSS and submission of compliance reports to the acquiring bank and/or card payment brands



- Reference https://www.pcisecuritystandards.org/pdfs/pcissc_getting_started_with_pcidss.pdf

VISA – Merchant Validation Requirements

Level / Tier	Merchant Criteria	Validation Requirements
1	Merchants processing over 6 million Visa transactions annually (all channels) **or** Global merchants identified as Level 1 by any Visa region	Annual Report on Compliance ("ROC") by Qualified Security Assessor ("QSA") •Quarterly network scan by Approved Scan Vendor ("ASV") •Attestation of Compliance Form
2	Merchants processing 1 million to 6 million Visa transactions annually (all channels)	Annual Self-Assessment Questionnaire ("SAQ") •Quarterly network scan by ASV •Attestation of Compliance Form
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually	Annual SAQ •Quarterly network scan by ASV •Attestation of Compliance Form
4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually	Annual SAQ recommended •Quarterly network scan by ASV if applicable •Compliance validation requirements set by acquirer

- Reference http://www.visa-asia.com/ap/sea/mediacenter/pressrelease/NR_SGP_111108.shtml

VISA – Service Provider Validation Requirements

Level	All Regions	Validation Requirements	Result
1	VisaNet processors or any service provider that stores, processes and / or transmits over 300,000 transactions per year	Annual ROC by QSA •Quarterly network scan by ASV •Attestation of Compliance Form	Included on Visa's list of compliant Service Providers
2	Any service provider that stores, processes and / or transmits less than 300,000 transactions per year	Annual SAQ •Quarterly network scan by ASV •Attestation of Compliance Form	Not included on Visa's list / Confirmation Letter of Receipt [2]

- Registry of PCI DSS Compliant Service Providers Program:
  - www.visa-asia.com/spregistry
  - http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf
- Reference http://www.visa-asia.com/ap/sea/mediacenter/pressrelease/NR_SGP_111108.shtml

VISA – Summary of Aligned Framework by Date

Effective Date	Globally Aligned Mandate
February 1, 2009	Effective date for globally aligned Service Provider level definitions
September 30, 2009	**Acquirers must attest that Level 1 and 2 merchants do not retain prohibited payment card data subsequent to authorization of a transaction**
September 30, 2010	**PCI DSS compliance validation deadline for Level 1 merchants**

- Reference http://www.visa-asia.com/ap/sea/mediacenter/pressrelease/NR_SGP_111108.shtml

Links

- PCI Security Standards
  - https://www.pcisecuritystandards.org/
  - https://www.pcisecuritystandards.org/education/webinars.shtml
- Account Information Security (AIS)
  - http://www.visa-asia.com/secured
- Registry of Service Providers
  - http://www.visa-asia.com/ap/sea/merchants/riskmgmt/vrsp_index.shtml

Links

- Payment card brand compliance programs:
  - American Express: www.americanexpress.com/datasecurity
  - Discover Financial Services: www.discovernetwork.com/resources/data/data_security.html
  - JCB International: www.jcb-global.com/english/pci/index.html
  - MasterCard Worldwide: www.mastercard.com/sdp
  - Visa Inc: www.visa.com/cisp (U.S.)