A Dive into Payment Card Industry (PCI)

By

Saumya Vishnoi

About me

- Working as Security Consultant in SISA information Security
- PCI-QSA

Why is this Important ?

- 2013– Year of Braches
- Biggest breaches–
  - Target credit card breach
  - US beauty products chain ’Sally Beauty’ breach
  - Adobe breach

Credit Card Information!!!!

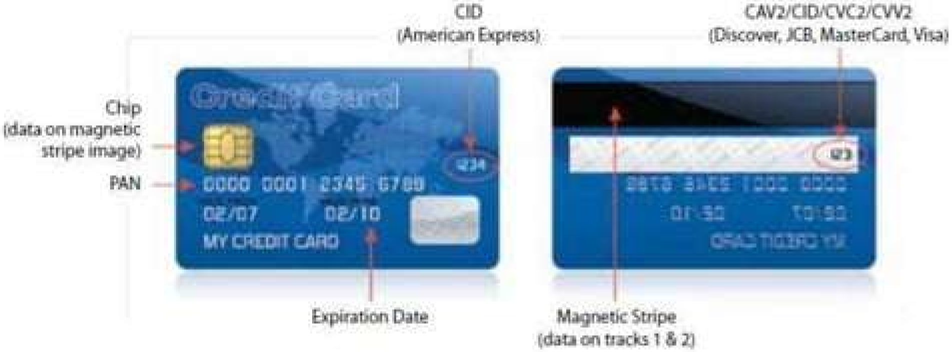
- Credit Card data is one of the most valuable target for cyber criminals

WHY ?

That is where the Money is ;)

Payment Card

Types of Data on a Payment Card

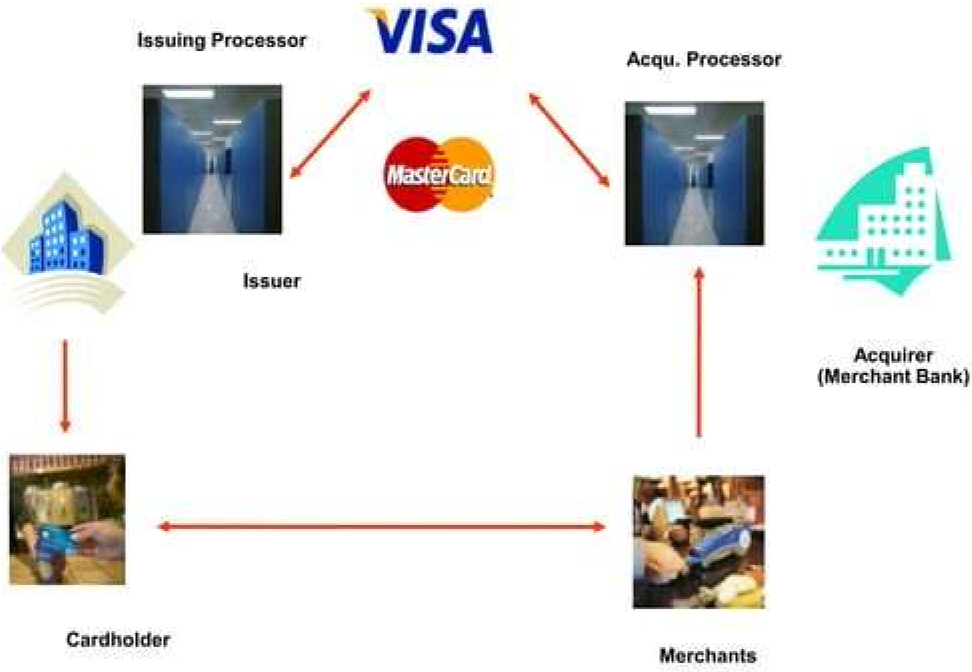


Payments Brands

Banks

- Issuer Bank
- Acquirer Bank

How a card Transaction Works ? (Card Present)



Issuing Processor

Acqu. Processor

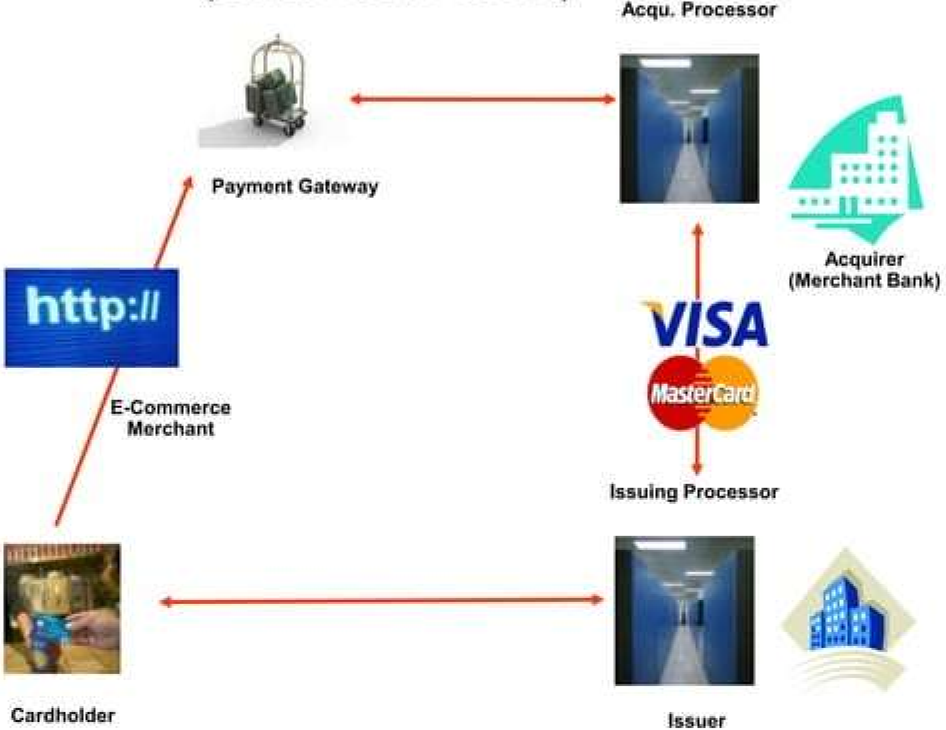
Issuer

Acquirer
(Merchant Bank)

Cardholder

Merchants

How a card Transaction Works ?
(Card Not Present)



Three Core Processing Actions

- Authentication
  - Validation of cardholders identity and card being used
- Authorization
  - Issuer approves or declines purchase
- Settlement
  - Transfer of funds into merchant account once product/service shipped or delivered

Protection of Card Information

PCI-SSC

- PCI Security Standard Council---

An independent industry standards body providing oversight of the development and management of Payment Card Industry Security Standards on a global basis.

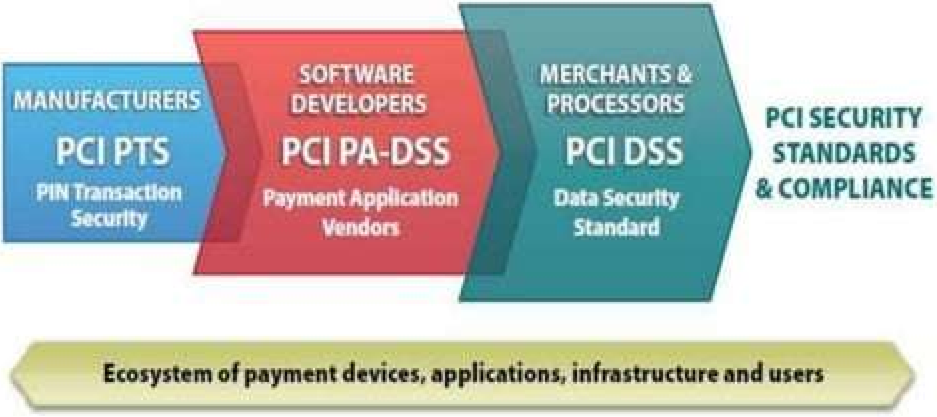
- Founded by ----

American Express, Discoverer Financial Services,

JCB International, MasterCard Worldwide, VISA Inc.

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data


MANUFACTURERS
PCI PTS
PIN Transaction Security
SOFTWARE DEVELOPERS
PCI PA-DSS
Payment Application Vendors
MERCHANTS & PROCESSORS
PCI DSS
Data Security Standard
PCI SECURITY STANDARDS & COMPLIANCE
Ecosystem of payment devices, applications, infrastructure and users

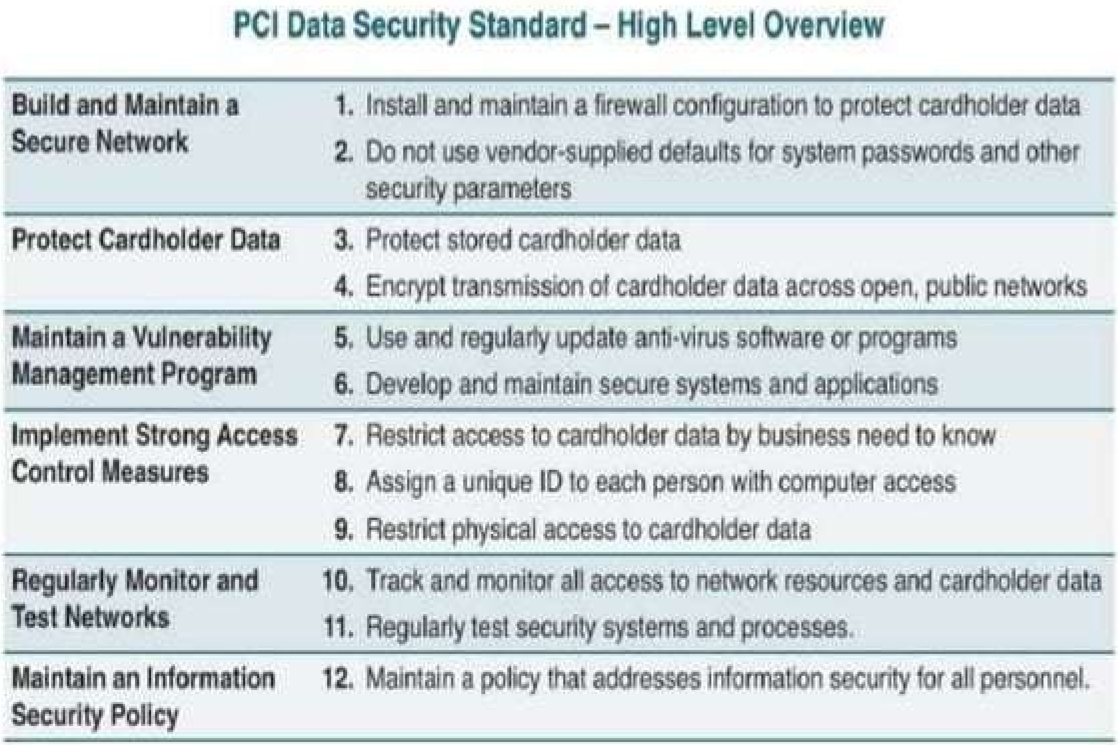
PCI-PTS

- PCI Pin Transaction Security
- Set of security requirements focused on characteristics and management of devices related to payment processing activities.
- For manufactures to be followed during the design, manufacture and transport of the device.

PA-DSS

- Payment Application Data Security Standard
- For only software applications that store, process or transmit card holder data as part of authorization and settlement.
- Applied to only off the shelf sold application

PCI DSS
Data Security Standard



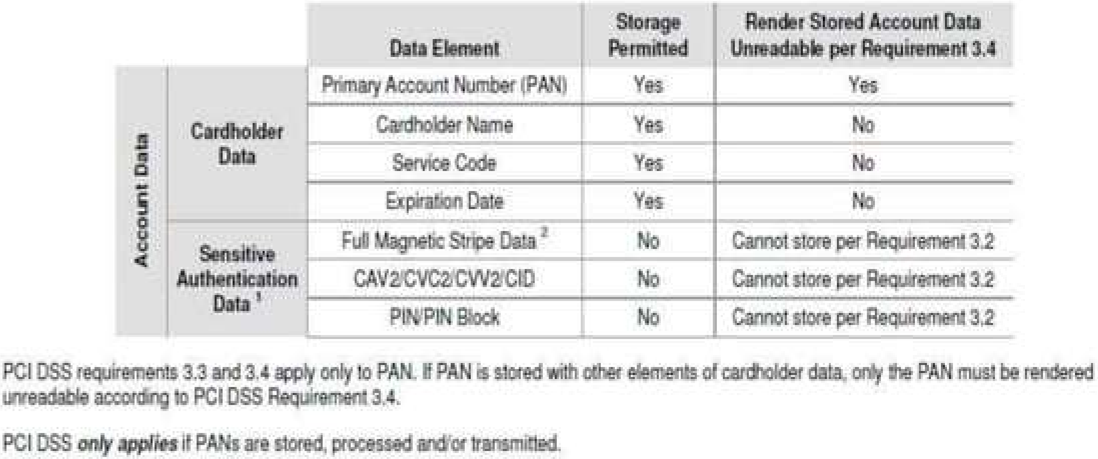
PCI Data Security Standard – High Level Overview

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 cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 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 for all personnel.

PCI DSS Applicability

- It applies to-
  - Systems that Store, Process and Transmit Card holder data
  - Systems that provide security services or may impact the security of Card Data Environment (CDE)
  - Any other Components or devices located within or connected to CDE

Card Holder Data



		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data[1]	Full Magnetic Stripe Data[2]	No	Cannot store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN Block	No	Cannot store per Requirement 3.2

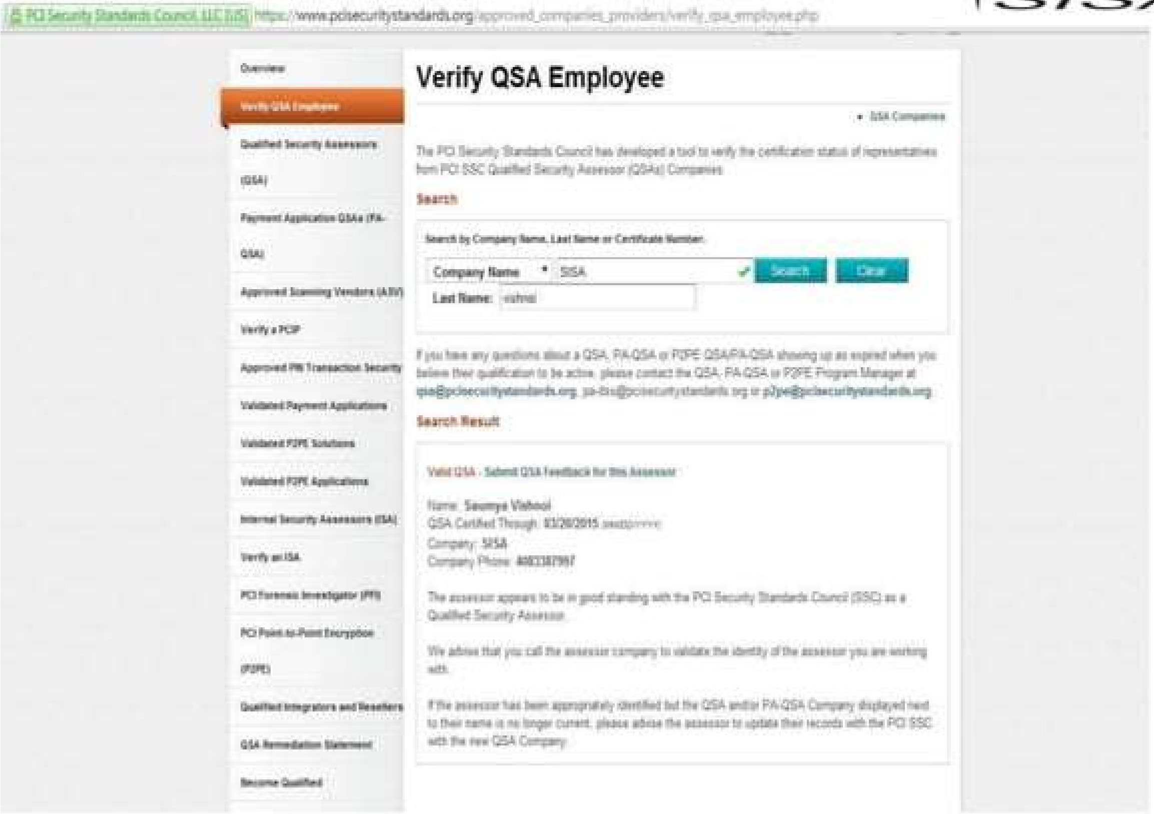
PCI DSS requirements 3.3 and 3.4 apply only to PAN. If PAN is stored with other elements of cardholder data, only the PAN must be rendered unreadable according to PCI DSS Requirement 3.4.

PCI DSS ***only applies*** if PANs are stored, processed and/or transmitted.

PCI-DSS Assessments

- Qualified Assessors:

- Self-Assessments Questionnaire:


PCI Security Standards Council, LLC [US]
https://www.pcisecuritystandards.org/approved_companies_providers/verify_qsa_employee.php
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
• QSA Companies
Search
Clear

Verify QSA Employee

The PCI Security Standards Council has developed a tool to verify the certification status of representatives from PCI SSC Qualified Security Assessor (QSAs) Companies

Search

Search by Company Name, Last Name or Certificate Number

Company Name * SISA

Last Name: vishnoi

If you have any questions about a QSA, PA-QSA or P2PE QSA/PA-QSA showing up as expired when you believe their qualification to be active, please contact the QSA, PA-QSA or P2PE Program Manager at qsa@pcisecuritystandards.org, pa-dss@pcisecuritystandards.org or p2pe@pcisecuritystandards.org

Search Result

Valid QSA - Submit QSA Feedback for this Assessor

Name: Saumya Vishnoi
QSA Certified Through: 03/28/2015 (mm/dd/yyyy)
Company: SISA
Company Phone: 4083387997

The assessor appears to be in good standing with the PCI Security Standards Council (SSC) as a Qualified Security Assessor.

We advise that you call the assessor company to validate the identity of the assessor you are working with.

If the assessor has been appropriately identified but the QSA and/or PA-QSA Company displayed next to their name is no longer current, please advise the assessor to update their records with the PCI SSC with the new QSA Company.

Global Merchant Levels

Level	American Express	MasterCard	Visa
1	Merchants processing 2.5 million American Express Card transactions annually or any merchant that American Express otherwise deems a Level 1.	Merchants processing over 6 million MasterCard transaction (all channels) annually, identified by another payment card brand as Level 1 or compromised merchants	Large Merchants processing over 6,000,000 Visa transactions annually (all channels), or global merchants identified as Level 1 by any VISA region.
2	Merchants processing 50,000 to 2.5 million American Express transactions annually or any merchant that American Express otherwise deems a Level 2	Merchants processing 1 million to 6 million MasterCard transactions annually All Merchants meeting the Level 2 criteria of competing payment brand	Merchants processing 1 million to 6 million Visa Transactions annually (all channels).
3	Merchants processing less than 50,000 American Express transaction annually	Merchants processing over 20,000 MasterCard e-commerce transactions annually. All Merchants meeting the level 3 criteria of competing brand	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually.
4	N/A	All other MasterCard merchants	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million transactions annually

Requirement 1

Install and maintain a firewall configuration to protect cardholder data

- Firewall and Router hardening
- Firewall rule review
- Firewall rule justification

Requirement 2

Do not use vendor-supplied defaults for system passwords and other security parameters

- Removal of defaults– settings, credentials
- Hardening
- Encrypted non-console access

Requirement 3

Protect stored cardholder data

- Storage of card holder data
- Not storing sensitive authentication data*
- Security of data while storage
- Masking of PAN*

Requirement 4

Encrypt transmission of cardholder data across open, public networks

- Secure transmission – wired
- Secure transmission – wireless
- End user messaging

Requirement 5

Protect all systems against malware and regularly update anti-virus software or programs

- Anti-Virus
- Update and scan settings
- Logs –generated , stored

Requirement 6

Develop and maintain secure systems and applications

- Risk ranking
- Patching
- Change Control
- Secure development
- Web Application Firewall

Requirement 7

Restrict access to cardholder data by business need to know

- Access rights assigned on need to know basis
- User creation and deletion process

Requirement 8

Identify and authenticate access to system components

- Unique user ID
- User access review
- 2-factor authentication for remote access

Requirement 9

Restrict physical access to cardholder data

- Physical access control
- CCTV
- Visitor Policy
- Physical security of Media
- Secure Destruction of Media
- Protecting POS devices from tempering

Requirement 10

Track and monitor all access to network resources and cardholder data

- Enable Logs
- Time synchronization
- FIM on logs
- Log review
- Retention period

Requirement 11

Regularly test security systems and processes

- Wireless scan
- Internal VA
- Internal PT
- External VA
- External PT
- Application Testing
- FIM

Requirement 12

Maintain a policy that addresses information security for all personnel

- Information Security Policy
- Risk assessment
- Awareness training
- Background verification

References

- PCI_DSS Requirements and Security Assessment Procedure version 2.0
- PCI_DSS Requirements and Security Assessment Procedure version 3.0
- PCI Quick Reference Guide

Questions ?

Thank You

saum98@gmail.com