PCI Security Standards Council™

QUALIFIED SECURITY ASSESSOR

Introduction to PCI Data Security Standards (DSS) and Compliance Processes

Trust earned.

FreedMaxick™

Contents

- PCI Data Security Standard (DSS)
- Report On Compliance (ROC) process
- Self-Assessment Questionnaire (SAQ) process
- External network security scan requirements
- Payment Application Data Security Standard (PA-DSS)
- Compensating controls
- Common issues clients could encounter

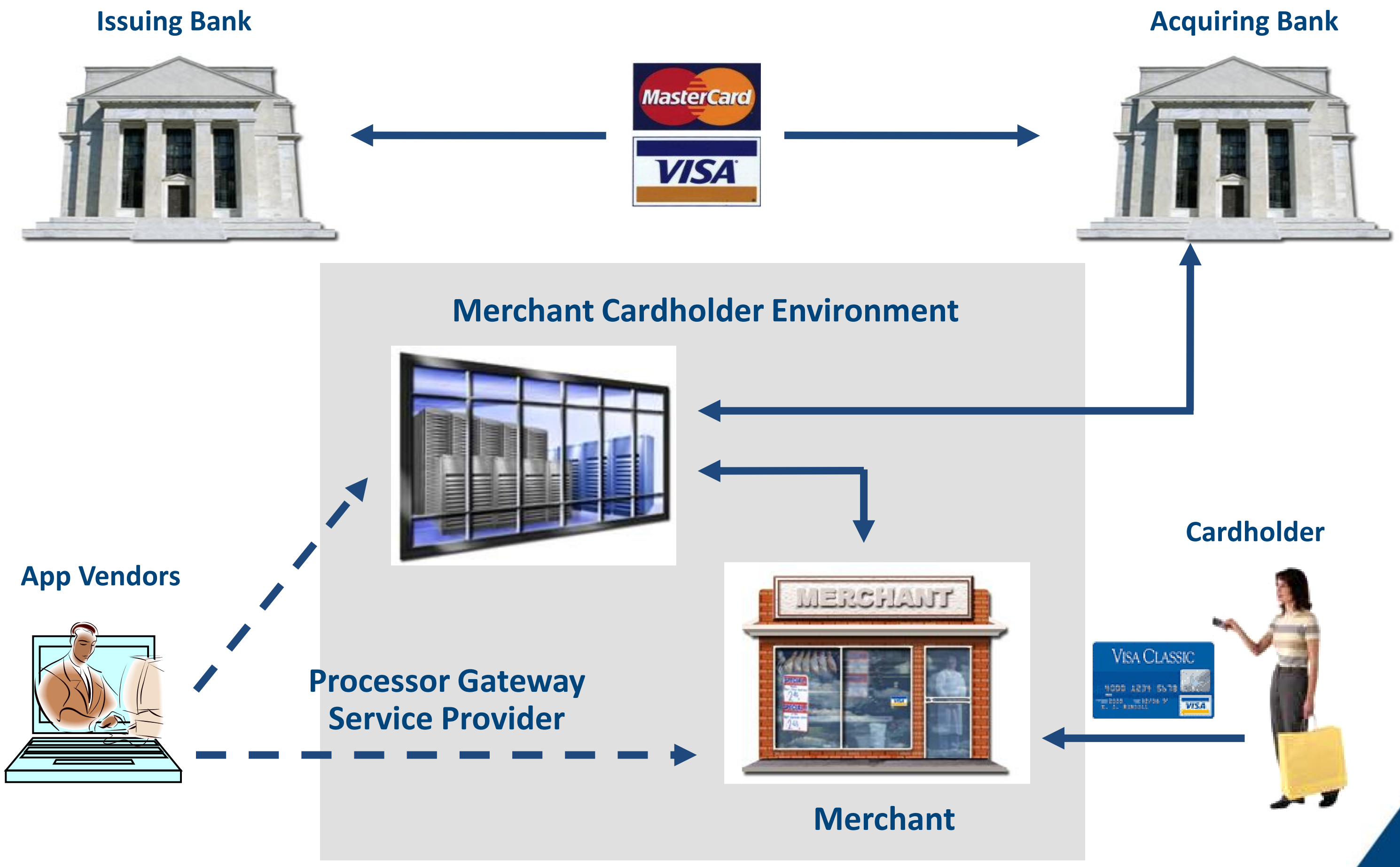
PCI DSS
Payment Card Industry Data Security Standard

- Standard that is applied to:
  - Merchants
  - Service providers (Banks, third-party vendors, gateways)
  - Systems (Hardware, software)

- That:
  - Stores cardholder data
  - Transmits cardholder data
  - Processes cardholder data

- Applies to:
  - Electronic transactions
  - Paper transactions

PCI Relationship Matrix



Issuing Bank

Acquiring Bank

Merchant Cardholder Environment

Cardholder

App Vendors

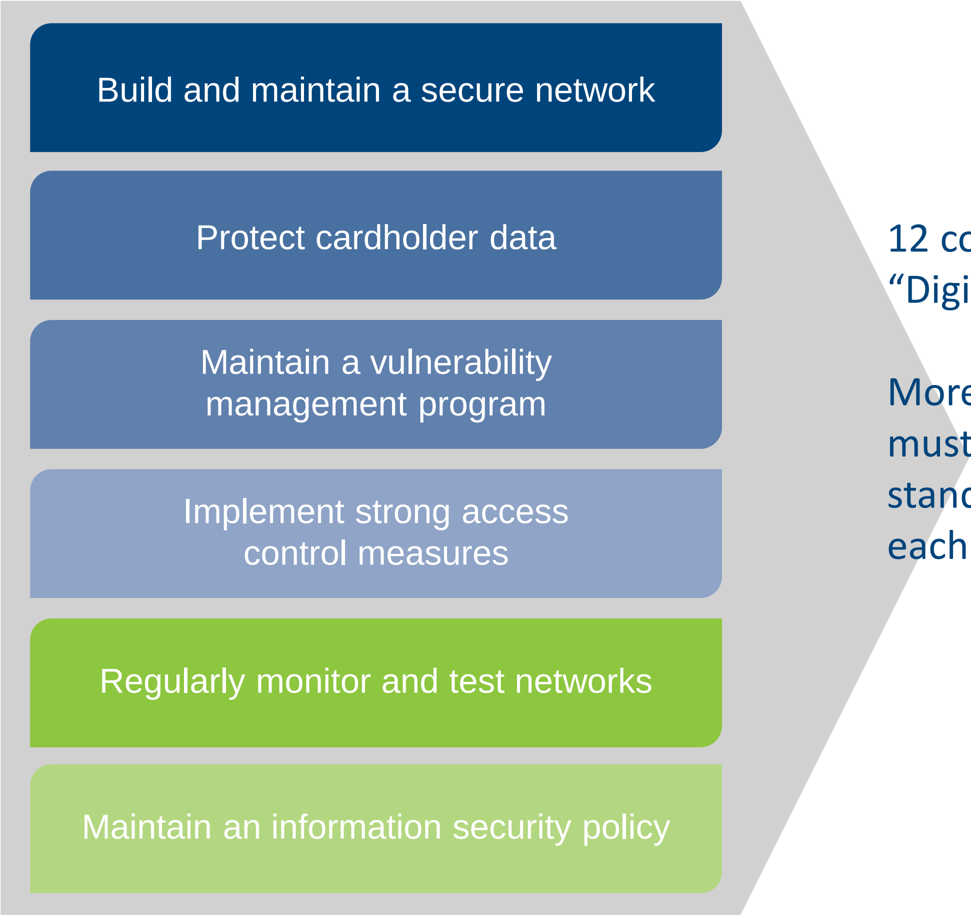
Processor Gateway
Service Provider

Merchant

PCI Standards

- Data Security Standard (DSS)
- Report On Compliance (ROC) process
- Self-Assessment Questionnaires (SAQ) process
- External network security scan requirements
- Payment Application Data Security Standard (PA-DSS)

PCI Data Security Standard



Build and maintain a secure network

Protect cardholder data

Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

12 control objectives known as the "Digital Dozen"

More than 218 control activities that must be tested with a "no fail" standard for any control activity for each of the 12 control objectives

PCI Data Security Standard (DSS)

Within the six domains, there are 12 requirements

- Build and maintain a secure network (40 questions)
  - **Requirement 1** - Install and maintain a firewall configuration to protect data
  - **Requirement 2** - Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect cardholder data (32 questions)
  - **Requirement 3** - Protect stored data
  - **Requirement 4** - Encrypt transmission of cardholder data and sensitive information across public networks

PCI Data Security Standard (DSS)

Within the six domains, there are 12 requirements

- Maintain a vulnerability management program (31 questions)
  - **Requirement 5** - Use and regularly update anti-virus software
  - **Requirement 6** - Develop and maintain secure systems and applications

PCI Data Security Standard (DSS)

Within the six domains, there are 12 requirements

- Implement “strong” access control measures (53 questions)
  - **Requirement 7** - Restrict access to data by business need-to-know
  - **Requirement 8** - Assign a unique identifier to each person with computer access
  - **Requirement 9** - Restrict physical access to cardholder data

PCI Data Security Standard (DSS)

Within the six domains, there are 12 requirements

- Regularly monitor and test networks (35 questions)
  - **Requirement 10** - Track and monitor all access to network resources and cardholder data
  - **Requirement 11** - Regularly test security systems and processes
- Maintain an information security policy (40 questions)
  - **Requirement 12** - Maintain a policy that addresses information security

Report On Compliance (ROC) Process

- Typically conducted by a QSA
- Can be conducted by an internal audit group with a Officer of the organization signing the document. Issues we typically encounter with this approach:
    - Internal audit did not have the technical expertise
    - Internal audit did not understand the process
    - Internal audit did not understand what constitutes proper supporting documentation for proving compliance

Self-Assessment Questionnaire (SAQ) Process

SAQ VALIDATION TYPE	DESCRIPTION	SAQ
1	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.	A
2	Imprint-only merchants with no electronic cardholder data storage	B
3	Merchants with web based virtual terminals, no electronic cardholder data storage	C-VT
4	Merchants with POS systems connected to the Internet, no electronic cardholder data storage	C
5	All other merchants (not included in Types 1-4 above) and all service providers defined by a payment brand as eligible to complete an SAQ.	D

SAQ A

- Simplest SAQ of all
- Only covers the following DSS requirements
  - Requirement 9 – Restrict physical access to cardholder data
  - Requirement 12 – Maintain a policy that addresses information security for employees and contractors

SAQ B

Have to comply with 5 of the 12 DSS requirements

- Requirement 3 - Protect stored cardholder data
- Requirement 4 - Encrypt transmission of cardholder data across open, public networks
- Requirement 7 - Restrict access to cardholder data by business need to know
- Requirement 9 - Restrict physical access to cardholder data
- Requirement 12 - Maintain a policy that addresses information security for employees and contractors

SAQ C-VT

Have to comply with 9 of 12 of the DSS requirements

- However, only have to comply with a select number of relevant requirements within each of the domains

SAQ C

Have to comply with all 12 of the DSS requirements

- However, only have to comply with a select number of relevant requirements within each of the domains

SAQ D

Basically a scaled back ROC

- All requirements are covered in various levels of detail

External Network Security Scan Requirements

- Must be conducted by an ASV
- Only necessary to test network components that face the Internet that process, store and / or transmit cardholder data

Payment Application Data Security Standard (PA-DSS)

What it is

- Certification for any application that processes, stores or transmits credit card data
- Applies only to a specific version of the application
- Certifies that the application complies with the concepts of the PCI DSS
- Certifies that cardholder data is properly processed, stored and / or transmitted by the application

Payment Application Data Security Standard (PA-DSS)

What it is NOT

- Does NOT guarantee compliance with the PCI DSS when the application is implemented
  - Need to read the application's implementation guide or similar documentation to determine what PCI DSS issues may still have to be managed by you as part of or after implementation of the application
- Application can still be storing cardholder data
  - PA-DSS (or PABP) compliance only assures you that the data is properly protected by encryption and other methods

Beware….

BEWARE – some application vendors believe that PA-DSS compliance gets them off the hook regarding PCI DSS compliance. This is not true.

Compensating Controls

As defined by the PCI SSC

- "Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints but has sufficiently mitigated the risk associated with the requirement through implementation of other controls."

PCI DSS Exempt Myth

- All organizations that store, transmit or process cardholder data are subject to the standard and to card association rules
  - **No exemption provided to anyone**
- Immunity does not apply because
  - Requirement is contractual - not regulatory or statutory
  - Card associations can be selective who they provide services to
  - Merchants accept services on a voluntary basis
  - Merchants agree to abide by association rules when they execute e-merchant bank agreement
- Merchant banks are prohibited by association rules from indemnifying a merchant from not being compliant with the standard
- Association Rules require merchant banks to monitor merchants to ensure their compliance
  - Failure of a merchant bank to require compliance jeopardizes the merchant bank's right to continue to be a merchant bank
  - Any fines levied are against the merchant bank, which in turns passes the fines onto the merchant

Common Issues Clients Could Encounter

- Scope of assessment
  - Network not properly segmented
  - Knowledge of what applications process, store and / or transmit cardholder data
    - Paper records
    - Facsimile machine(s)
    - Centralized electronic facsimile system
    - Electronic mail system
    - Document management system

Common Issues Clients Could Encounter

"It was compliant last year."

- PCI standards are constantly being interpreted by the card brands based on current threats
    - PCI SSC does put their clarification responses to questions on their Web site
- What is compliant this year may not be compliant next year or even next week
- Consistency between QSAs

Have Questions About PCI Compliance?
Need PCI Compliance Audit Assistance?

Contact us here, or

Call Larry Hessney at (585) 360-1480

Trust earned.

FreedMaxick™

FREEDMAXICK.COM

PCI Security Standards Council™

QUALIFIED SECURITY ASSESSOR