WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

PCI Compliance

What Do Credit Unions Need to Know?

June 2019

Create Opportunities

We promise to know you and help you.

CLA – A Professional Services Firm

- A professional services firm with three distinct business lines
  - Wealth Advisory
  - Outsourcing
  - Audit, Tax, and Consulting

- More than 6,500 professionals
- Offices coast to coast
- Serve more than 1,500 financial institutions

Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC.

Cyber Security Services

Information Security offered as specialized service offering for over 20 years

- Largest Credit Union Service Practice*

- Penetration Testing and Vulnerability Assessment
  - Black Box, Red Team, and Collaborative Assessments
- IT/Cyber security risk assessments
- IT audit and compliance (GLBA, FFIECI, CIS, etc…)
- **PCI-DSS Readiness and Compliance Assessments**
- Incident response and forensics
- Independent security consulting
- Internal audit support

AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports ®

PCI Security Standards Council ®

HITRUST
Authorized CSF Assessor

- **At last count… CLA was one of only 5 firms in the nation with all three of these designations/affiliations/capabilities**

*Callahan and Associates 2018 Guide to Credit Union CPA Auditors.

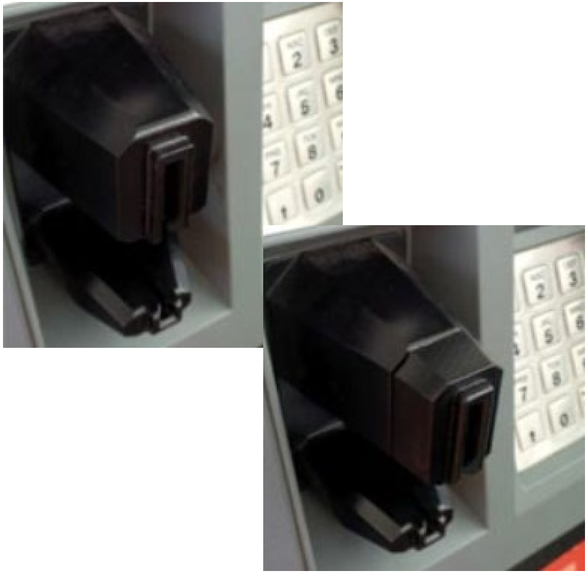
C:\whoami

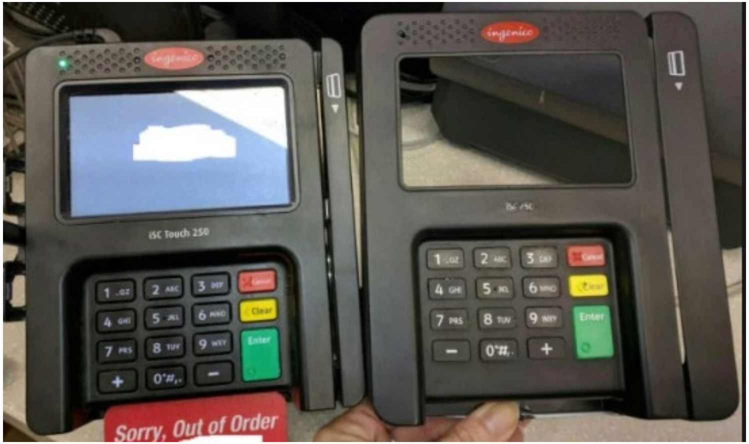
- “Professional Student”
- Science Teacher / Self Taught Computer Guy
- IT Consultant - Project Manager – IT Staff/Help Desk - Hacker
- Assistant Scout Master (Boy Scouts)

2018 Breaches That Included Payment Cards

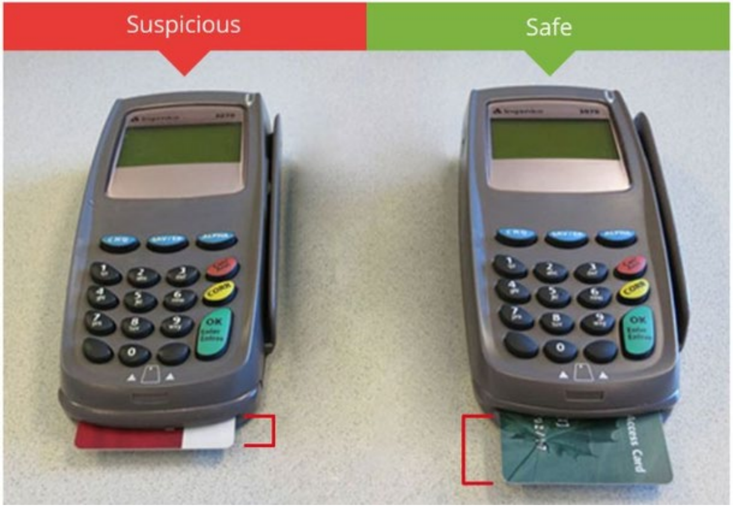
LAKE WORTH, Fla. -- Customers of the City of Lake Worth Utilities who utilized the online credit card payment option to pay their bill may have experienced a possible breach of their credit card information.

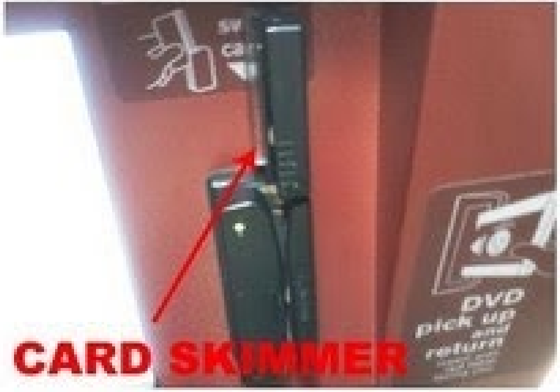
Skimmers - examples





Skimmers - examples

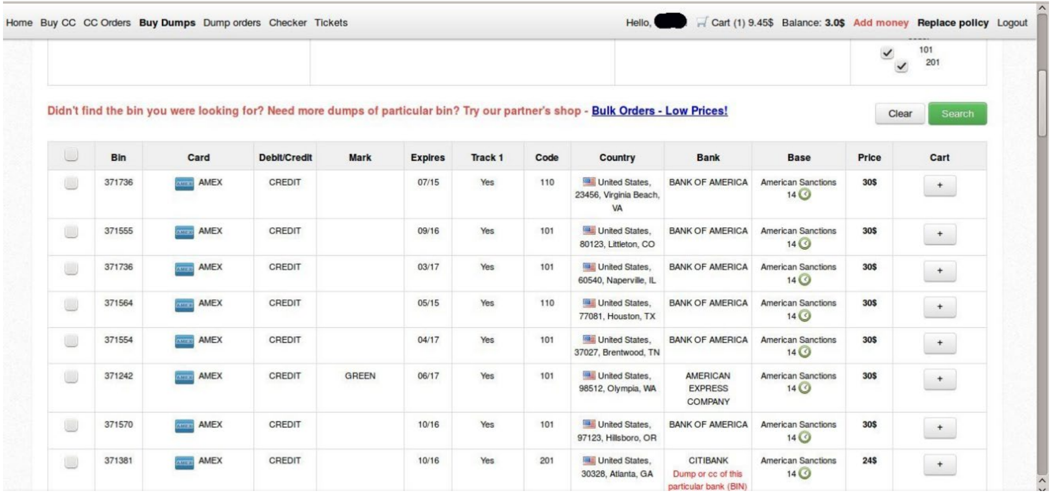




Marketplace for Stolen Information

Attackers buy and sell data on cyber black market

– “The Dark Web” - similar to amazon.com



Home Buy CC CC Orders Buy Dumps Dump orders Checker Tickets
Hello, [redacted] Cart (1) 9.45$ Balance: 3.0$ Add money Replace policy Logout
✓ 101
✓ 201
Clear
Search

Didn't find the bin you were looking for? Need more dumps of particular bin? Try our partner's shop - Bulk Orders - Low Prices!

□	Bin	Card	Debit/Credit	Mark	Expires	Track 1	Code	Country	Bank	Base	Price	Cart
□	371736	AMEX	CREDIT		07/15	Yes	110	United States, 23456, Virginia Beach, VA	BANK OF AMERICA	American Sanctions 14	30$	+
□	371555	AMEX	CREDIT		09/16	Yes	101	United States, 80123, Littleton, CO	BANK OF AMERICA	American Sanctions 14	30$	+
□	371736	AMEX	CREDIT		03/17	Yes	101	United States, 60540, Naperville, IL	BANK OF AMERICA	American Sanctions 14	30$	+
□	371564	AMEX	CREDIT		05/15	Yes	110	United States, 77081, Houston, TX	BANK OF AMERICA	American Sanctions 14	30$	+
□	371554	AMEX	CREDIT		04/17	Yes	101	United States, 37027, Brentwood, TN	BANK OF AMERICA	American Sanctions 14	30$	+
□	371242	AMEX	CREDIT	GREEN	06/17	Yes	101	United States, 98512, Olympia, WA	AMERICAN EXPRESS COMPANY	American Sanctions 14	30$	+
□	371570	AMEX	CREDIT		10/16	Yes	101	United States, 97123, Hillsboro, OR	BANK OF AMERICA	American Sanctions 14	30$	+
□	371381	AMEX	CREDIT		10/16	Yes	201	United States, 30328, Atlanta, GA	CITIBANK Dump or cc of this particular bank (BIN)	American Sanctions 14	24$	+

Exercise

- Normally a 5 Minute exercise…
- Describe how your organization stores, processes, or transmits credit card information
- Think in terms of the steps/stages followed
  - Examples:
    - ◊ Accept payment information over the phone
    - ◊ Members make payments online
    - ◊ Receive payment information in the mail
    - ◊ Member statements are sent/stored/reviewed by member services reps
- End Goal is to understand "where the card data lives"

Exercise – QUESTIONS

- Do you accept CC payment “in-person”?
- Do you accept CC payment over the phone?
- Do you accept CC payment via a website?
- Do you rely on a 3rd party/vendor to host or manage any of your data systems?
- Do you store or process CC data for someone else?
- Do you have instant issue capabilities?
- Are ATM machines “on your network”?

PCI - DSS Overview

A Long Time Ago…
In a Place Far Far Away…

Overview – PCI DSS

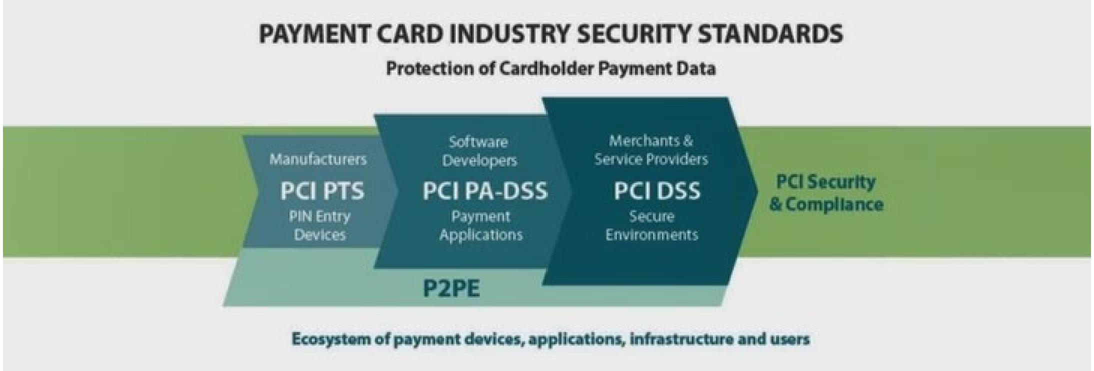
Each major card brand had its own separate criteria for implementing credit card security.

Merchants and processors who accepted multiple brands of cards needed to have a separate compliance program for each.

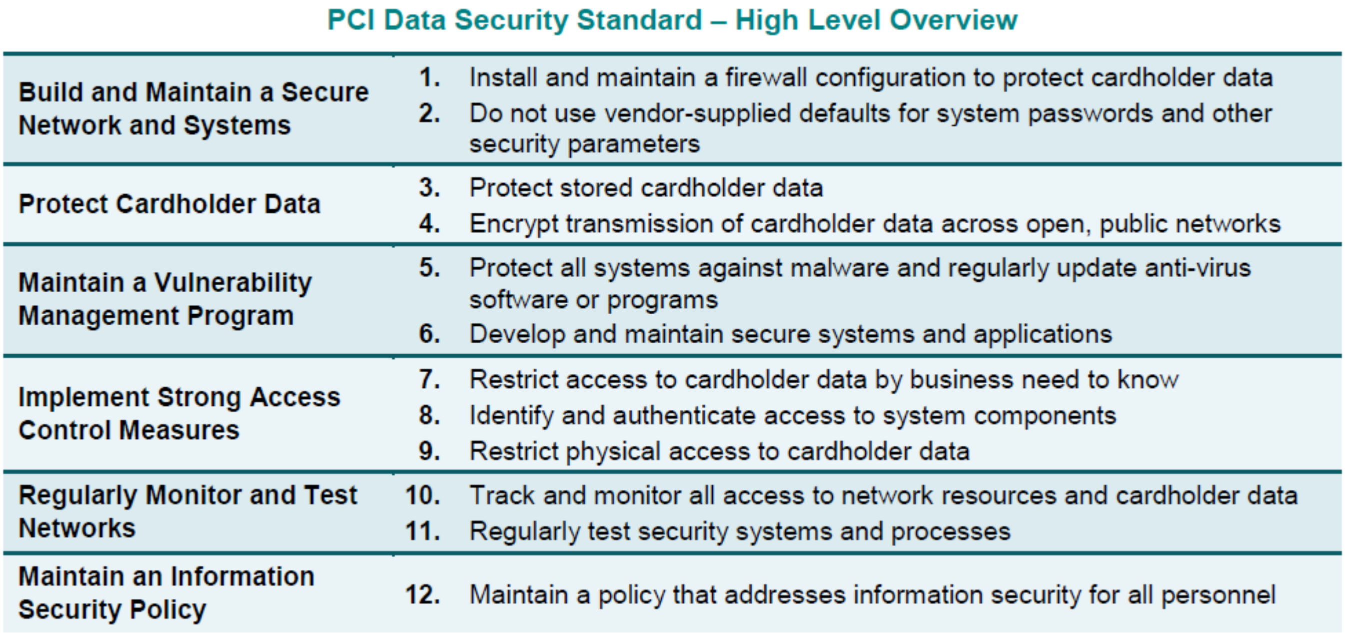
- Visa's Cardholder Information Security Program
- MasterCard's Site Data Protection
- American Express' Data Security Operating Policy
- Discover's Information Security and Compliance
- JCB's Data Security Program

The PCI Security Standards

- **In 2006**, the major payment card brands formed the Payment Card Industry Security Standards Council (PCISSC).
- This council developed and has continually updated the Data Security Standard (DSS) that all merchants must adhere to worldwide.
- The DSS is a set of 12 detailed requirements that ensure maximum payment card security.


PAYMENT CARD INDUSTRY SECURITY STANDARDS
Protection of Cardholder Payment Data
Manufacturers
PCI PTS
PIN Entry Devices
Software Developers
PCI PA-DSS
Payment Applications
Merchants & Service Providers
PCI DSS
Secure Environments
PCI Security & Compliance
P2PE
Ecosystem of payment devices, applications, infrastructure and users

PCI DSS Requirements
“The Digital Dozen”



PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	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. Protect all systems against malware 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. Identify and authenticate access to system components 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

Cardholder Data (CHD)

The PCI DSS defines CHD to be:

> "At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code."

- **PAN** – Acronym for "primary account number" and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account
- **Service Code** – Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.
- **SAD** – Acronym for "sensitive authentication data." Security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

Cardholder Data Environment (CDE)

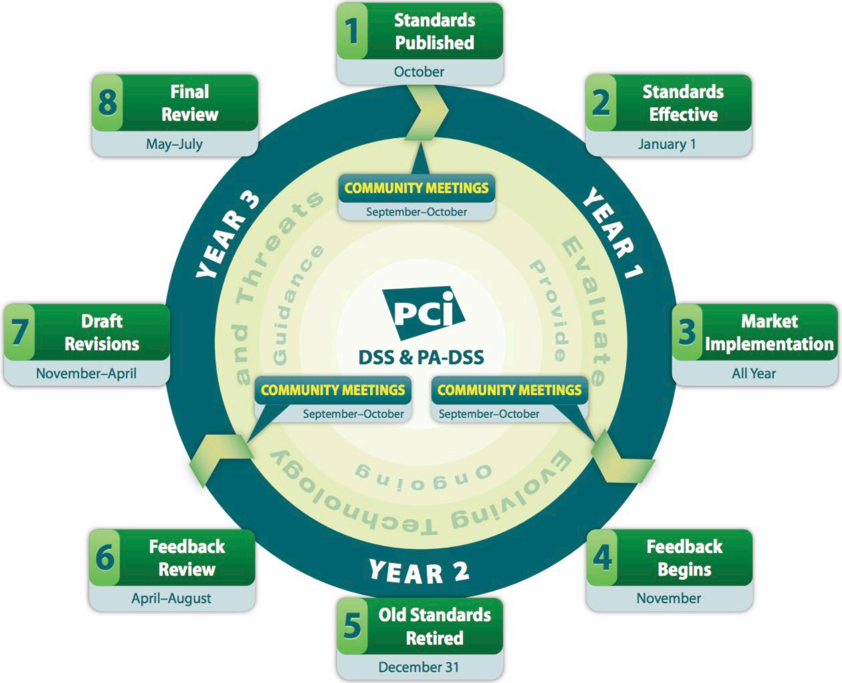
The PCI DSS defines the CDE to be "***the people, processes and technology*** that store, process or transmit cardholder data or sensitive authentication data, including any connected system components."

- **Store** – when cardholder data is inactive or at rest (e.g., located on electronic media, system component memory, paper, etc…)
- **Process** – when cardholder data is actively being used by a system component (e.g., entered, edited, manipulated, printed, viewed, etc…)
- **Transmit** – when cardholder data is being transferred from one location to another (e.g., data in motion)

PCI DSS Timeline

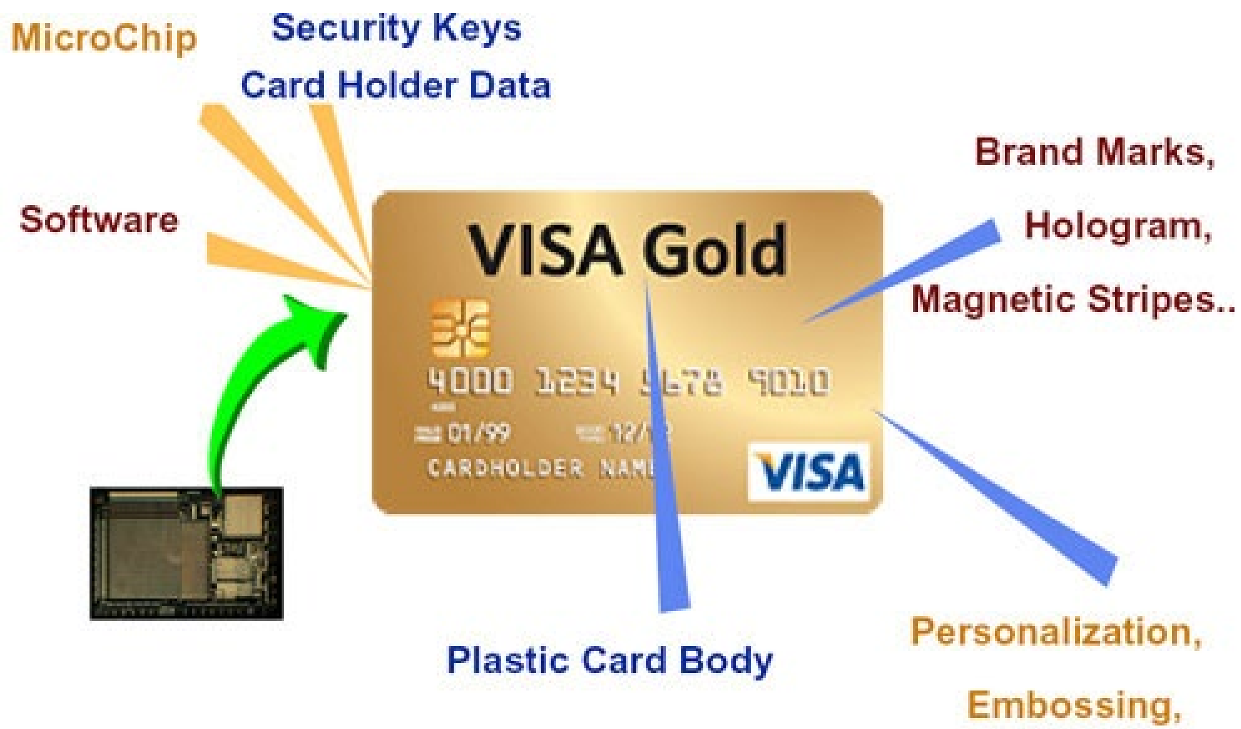
- Version 1.0 – December 15, 2004
- Version 1.1 – September 6, 2006
- Version 1.2 - October 1, 2008
- Version 2.0 – October 2010
- Version 3.0 – November 2013
- Version 3.1 – April 2015
- Version 3.2 – April 2016
- Version 3.2.1 – May 2018

Lifecycle Changes to PCI DSS



- https://www.pcisecuritystandards.org/pdfs/pci_lifecycle_for_changes_to_dss_and_padss.pdf

The Basics – Your Credit Card



MicroChip

Security Keys

Card Holder Data

Software

Brand Marks,

Hologram,

Magnetic Stripes..

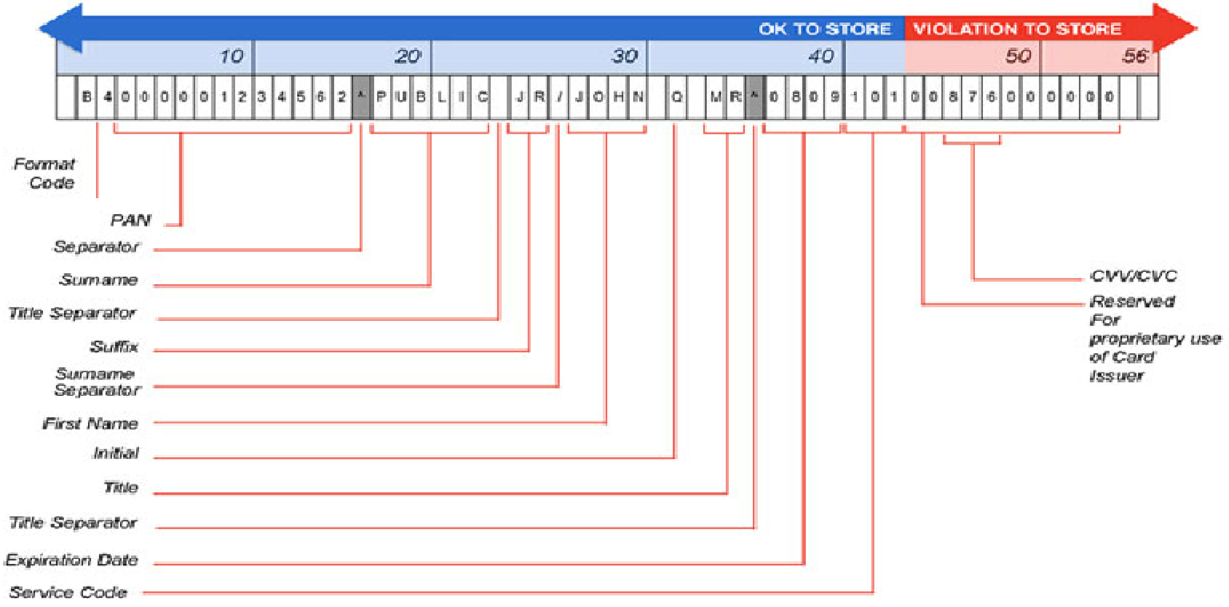
Plastic Card Body

Personalization,

Embossing,

The Basics – What is "Card Data"

Track 1 Data



The Basics – How Card Processing Works

Cardholder

Consumers purchasing goods either as a "Card Present" or "Card Not Present" transaction

Receives the payment card and bills from the issuer

Issuer

Bank or other organization issuing a payment card on behalf of a Payment Brand (e.g. MasterCard & Visa)

Payment Brand issuing a payment card directly (e.g. Amex, Discover, JCB)

Merchant

Organization accepting the payment card for payment during a purchase

Acquirer

Bank or entity the merchant uses to process their payment card transactions

Receive authorization request from merchant and forward to Issuer for approval

Provide authorization, clearing, and settlement services to merchants

Acquirer is also called:

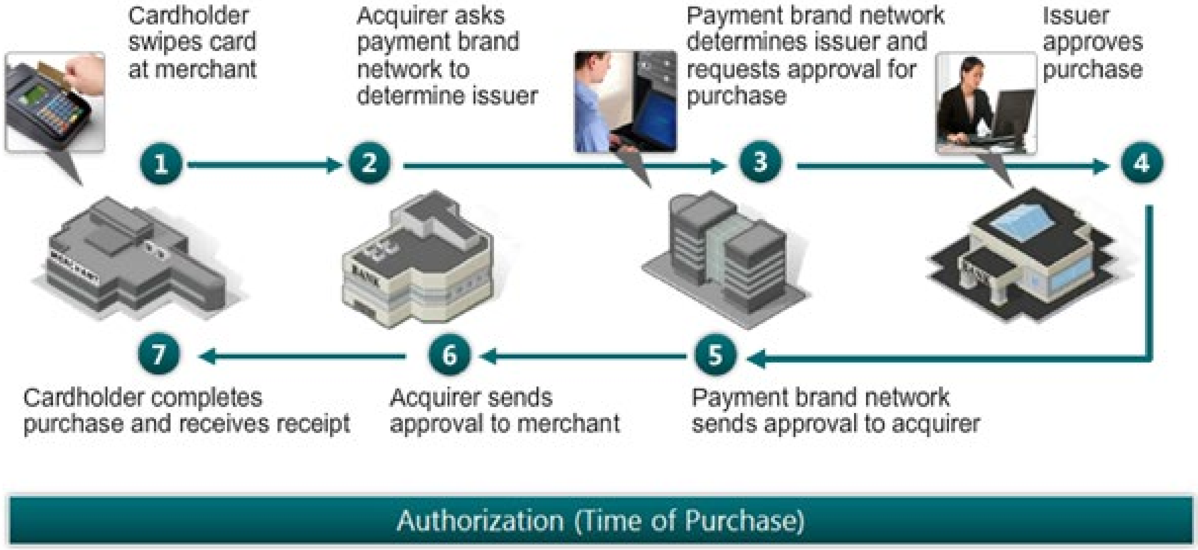
Merchant Bank

ISO (sometimes) independent sales organization

Payment Brand - Amex, Discover, JCB

Never Visa or MasterCard

The Basics - Authorization



1 Cardholder swipes card at merchant

2 Acquirer asks payment brand network to determine issuer

3 Payment brand network determines issuer and requests approval for purchase

4 Issuer approves purchase

5 Payment brand network sends approval to acquirer

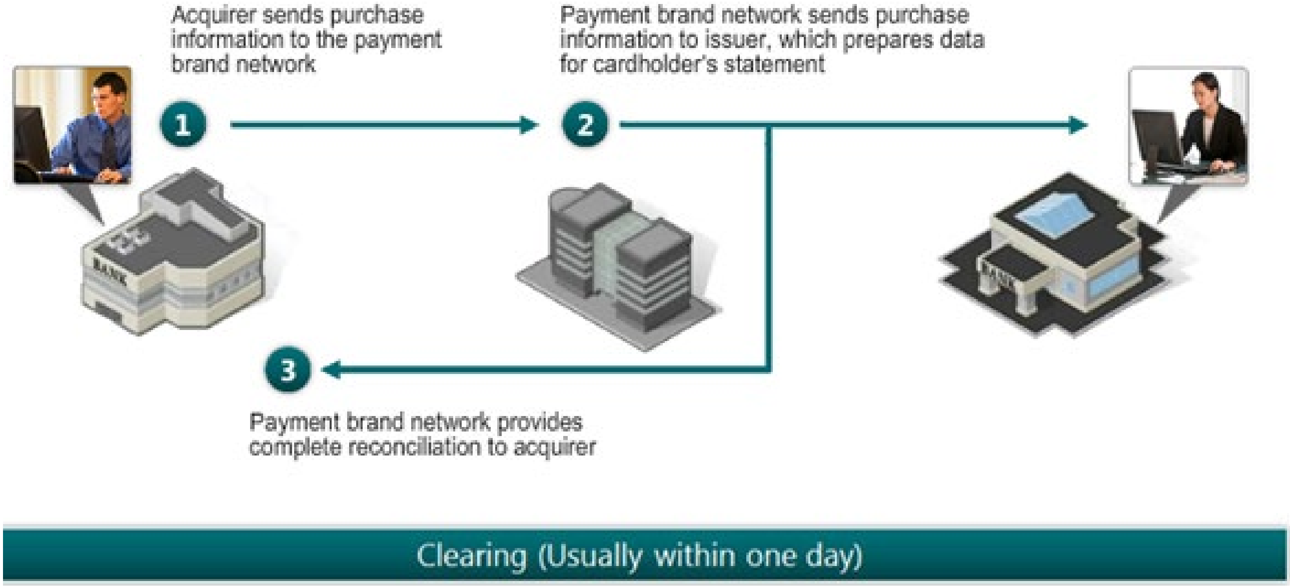
6 Acquirer sends approval to merchant

7 Cardholder completes purchase and receives receipt

Authorization (Time of Purchase)

- Merchant requests and receives authorization from the Issuer to allow the purchase to be conducted.
- Authorization Code is provided.

The Basics - Clearing



1 Acquirer sends purchase information to the payment brand network

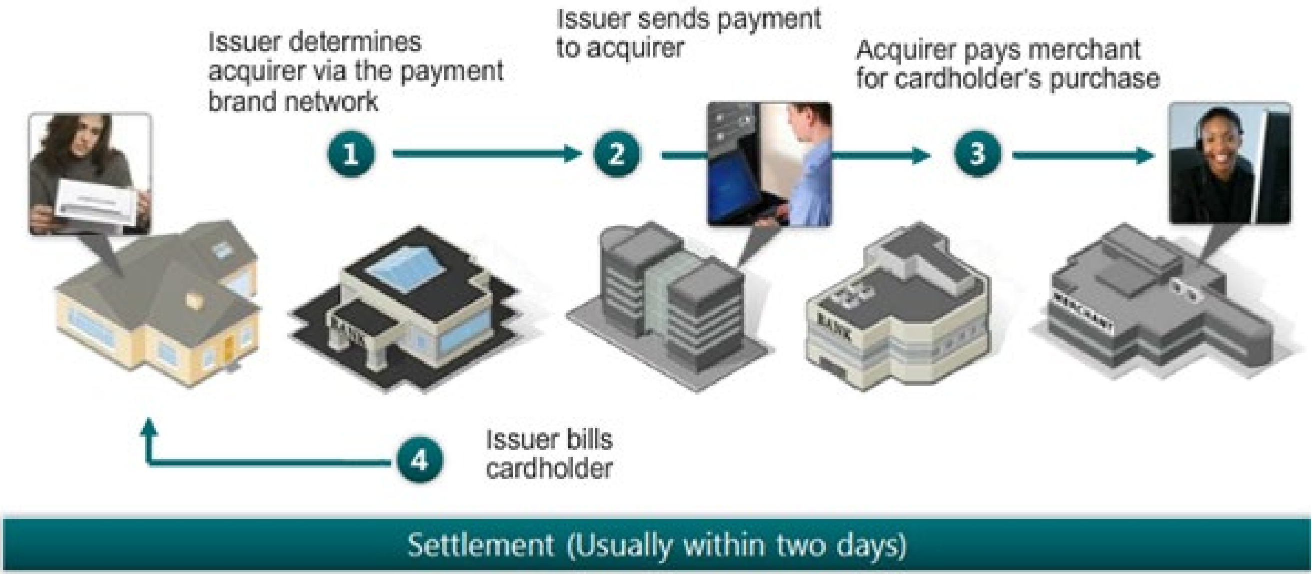
2 Payment brand network sends purchase information to issuer, which prepares data for cardholder's statement

3 Payment brand network provides complete reconciliation to acquirer

Clearing (Usually within one day)

- Acquirer and Issuer exchange purchase information

The Basics - Settlement



Issuer determines acquirer via the payment brand network

1

Issuer sends payment to acquirer

2

Acquirer pays merchant for cardholder's purchase

3

4

Issuer bills cardholder

Settlement (Usually within two days)

- Acquirer pays merchant for cardholder purchase
- Issuer bills cardholder

Merchants and Service Providers

- Merchant
  - Entity that accepts payment cards bearing the logos of any of the five members of PCI SSC as payment for goods and/or services.
- Service Provider
  - Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also includes companies that provide services that control or could impact the security of cardholder data.

PCI Merchant Levels

Merchant Level	**Merchant Definition**	**Compliance**
Level 1	More than 6 million V/MC transactions annually across all channels, including e-commerce	Annual Onsite PCI Data Security Assessment, Quarterly Network Scans, Annual External and Internal Penetration Testing
Level 2	1,000,000 – 5,999,999 V/MC transactions annually	Annual Self Assessment Questionnaire, Quarterly Network Scans, Annual External and Internal Penetration Testing
Level 3	20,000 – 1,000,000 V/MC **e-commerce transactions** annually	Annual Self Assessment Questionnaire, Quarterly Network Scans, Annual External and Internal Penetration Testing
Level 4	Less than 20,000 e-commerce V/MC transactions annually, and all merchants across channel up to 1,000,000 VISA transactions annually	Annual Self Assessment Questionnaire, Quarterly Network Scans, Annual External and Internal Penetration Testing

PCI Service Provider Levels

Service Provider Level	Service Provider Definition	Compliance
Level 1	VisaNet processors or any service provider that stores, processes and/or transmits over 300,000 transactions per year.	Annual Onsite PCI Data Security Assessment, Quarterly Network Scans, Annual External and Internal Penetration Testing, Quarterly Wireless Testing
Level 2	Any service provider that stores, processes and/or transmits less than 300,000 transactions per year.	Annual Self Assessment Questionnaire, Quarterly Network Scans, Annual External and Internal Penetration Testing, Quarterly Wireless Testing

Complying with PCI

Compliance VS. Certification (reporting)

Every organization that stores, processes, or transmits credit card data needs to comply with all DSS standards.

Depending on the type and size of the organization you must annually certify compliance utilizing either a self assessment questionnaire (SAQ) or independent third party review and Report on Compliance (ROC).

PCI DSS Self-Assessment Questionnaire (SAQ)

The PCI DSS SAQ consists of two components:

1. Questions corresponding to the PCI DSS requirements
   - Appropriate to service providers and merchants
2. Attestation of Compliance
   - Organization certification of eligibility to perform and have performed the appropriate Self-Assessment. The correct Attestation will be packaged with the SAQ selected.

Types of Self Assessment Questionnaires

There are eight SAQ categories:

A Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.

B Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic cardholder data storage

C-VT Merchants using **only web-based virtual terminals**, no electronic cardholder data storage

C Merchants with **payment application systems connected to the Internet**, no electronic cardholder data storage

D All other merchants not included in descriptions for SAQ types A through C above, and all service providers defined by a payment brand as eligible to complete an SAQ.

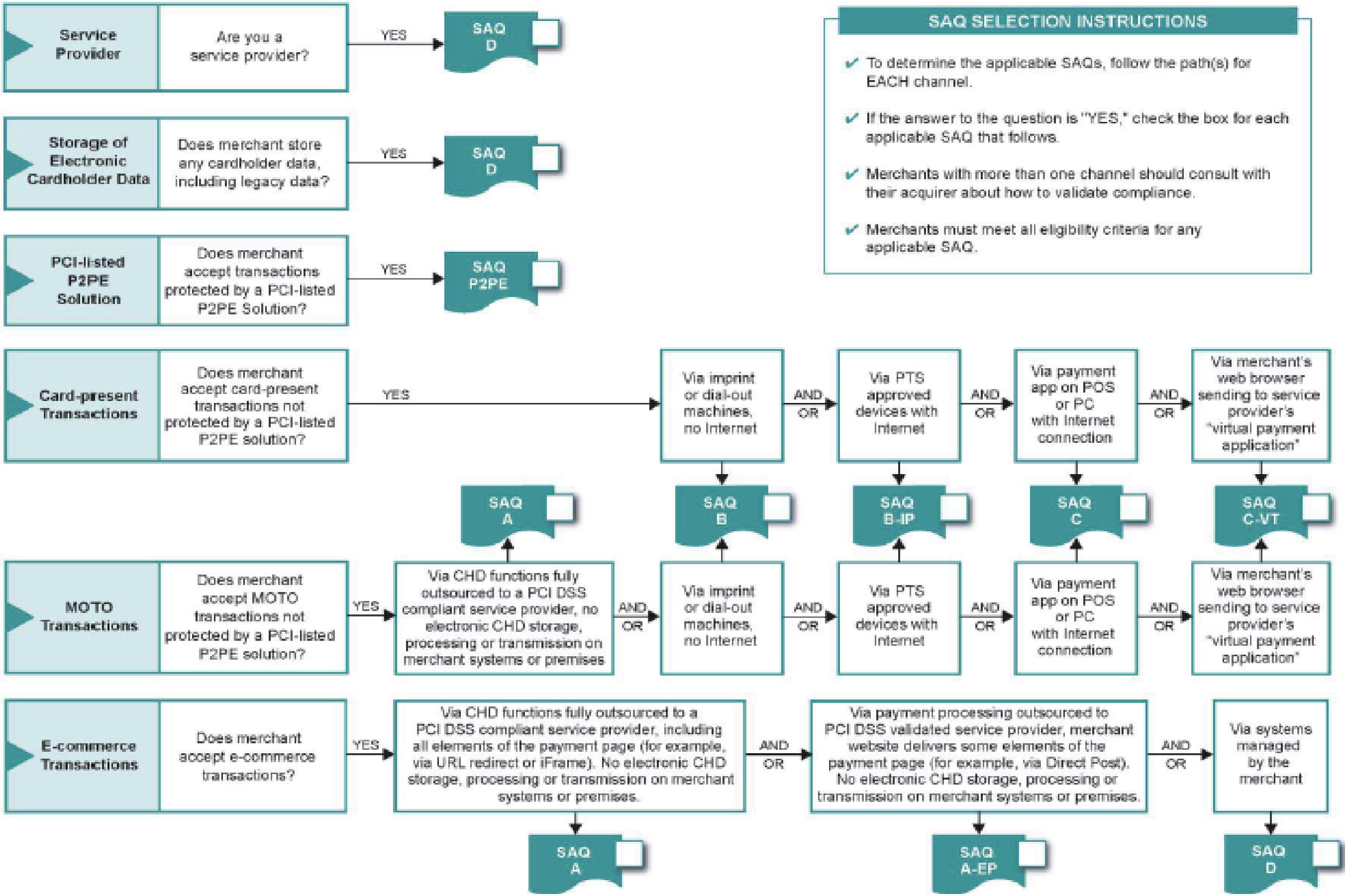
Types of Self Assessment Questionnaires

P2PE Merchants who have implemented a validated Point-to-Point Encryption Solution that is listed on the PCI SSC website (Not applicable to e-commerce channels)

A-EP E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchants systems or premises. (applicable only to e-commerce channels)

B-IP Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage.

Which SAQ Best Applies to My Environment?



SAQ SELECTION INSTRUCTIONS

- ✓ To determine the applicable SAQs, follow the path(s) for EACH channel.
- ✓ If the answer to the question is "YES," check the box for each applicable SAQ that follows.
- ✓ Merchants with more than one channel should consult with their acquirer about how to validate compliance.
- ✓ Merchants must meet all eligibility criteria for any applicable SAQ.

Service Provider – Are you a service provider? – YES → SAQ D □

Storage of Electronic Cardholder Data – Does merchant store any cardholder data, including legacy data? – YES → SAQ D □

PCI-listed P2PE Solution – Does merchant accept transactions protected by a PCI-listed P2PE Solution? – YES → SAQ P2PE □

Card-present Transactions – Does merchant accept card-present transactions not protected by a PCI-listed P2PE solution? – YES → Via imprint or dial-out machines, no Internet → SAQ B □ – AND/OR → Via PTS approved devices with Internet → SAQ B-IP □ – AND/OR → Via payment app on POS or PC with Internet connection → SAQ C □ – AND/OR → Via merchant's web browser sending to service provider's "virtual payment application" → SAQ C-VT □

MOTO Transactions – Does merchant accept MOTO transactions not protected by a PCI-listed P2PE solution? – YES → Via CHD functions fully outsourced to a PCI DSS compliant service provider, no electronic CHD storage, processing or transmission on merchant systems or premises → SAQ A □ – AND/OR → Via imprint or dial-out machines, no Internet → SAQ B □ – AND/OR → Via PTS approved devices with Internet → SAQ B-IP □ – AND/OR → Via payment app on POS or PC with Internet connection → SAQ C □ – AND/OR → Via merchant's web browser sending to service provider's "virtual payment application" → SAQ C-VT □

E-commerce Transactions – Does merchant accept e-commerce transactions? – YES → Via CHD functions fully outsourced to a PCI DSS compliant service provider, including all elements of the payment page (for example, via URL redirect or iFrame). No electronic CHD storage, processing or transmission on merchant systems or premises. → SAQ A □ – AND/OR → Via payment processing outsourced to PCI DSS validated service provider, merchant website delivers some elements of the payment page (for example, via Direct Post). No electronic CHD storage, processing or transmission on merchant systems or premises. → SAQ A-EP □ – AND/OR → Via systems managed by the merchant → SAQ D □

- https://www.pcisecuritystandards.org/documents/SAQ_InstrGuidelines_v3-1.pdf

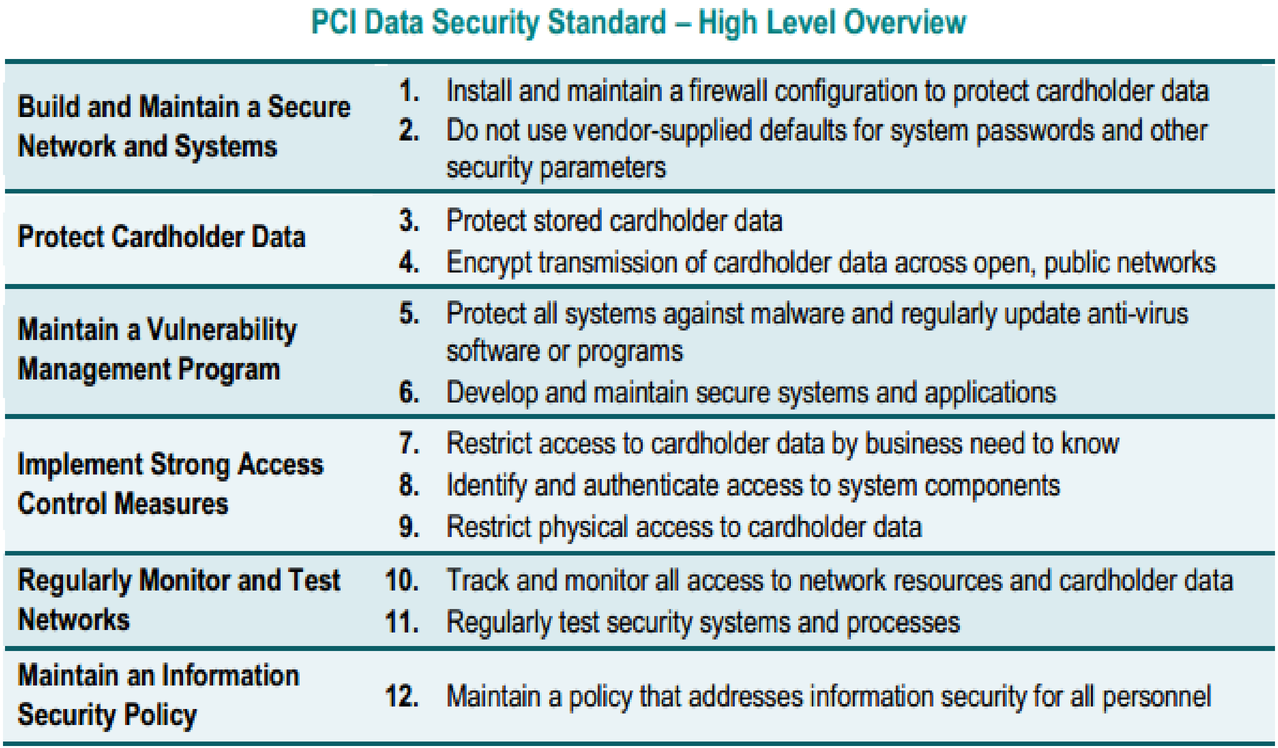
How to Scope a PCI DSS Assessment

How does the organization receive card holder data?	
How many applications store, process, or transmit cardholder data?	
How many databases platforms are used to store cardholder data (e.g. Oracle, MS SQL, DB2)?	
How many servers are used to store, process or transmit cardholder data?	
What are the operating systems for each of the servers (e.g. MS, UNIX, Linux, AS400, etc…)?	
Is there segmentation between the systems with cardholder data and the rest of the network?	
How is segmentation achieved (e.g. VLAN, Firewall, etc…)?	
How many Internet, DMZ, or segmentation firewalls are in place?	

How to Scope a PCI DSS Assessment

Is wireless technology in use anywhere on the network? If so, in how many locations?	
Is cardholder data transmitted over wireless devices at any point?	
Are payment card transactions accepted through a web server?	
Is PAN or other cardholder data stored on the POS systems for any length of time?	
How many data centers store, process or transmit cardholder data?	
How many call centers store, process or transmit cardholder data?	
Is any part of the environment outsourced?	
Are there third parties, outsourcers, or business partners connected to the network?	

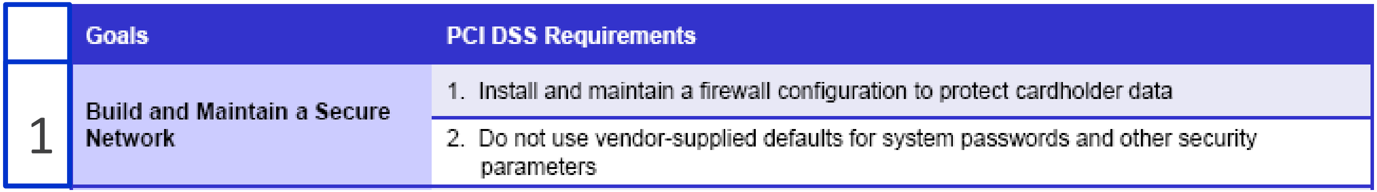
Overview – PCI DSS – "Digital Dozen"



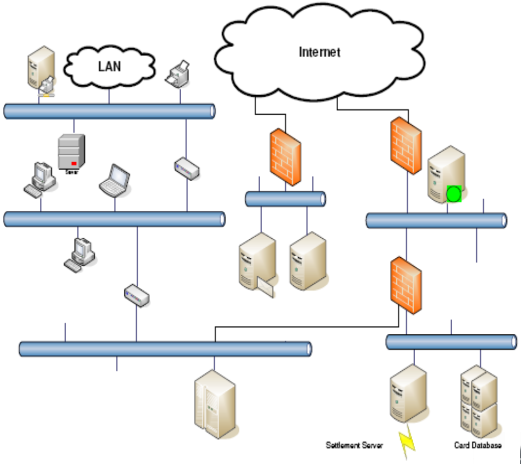
PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	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. Protect all systems against malware 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. Identify and authenticate access to system components 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 – Build & Maintain a Secure Network



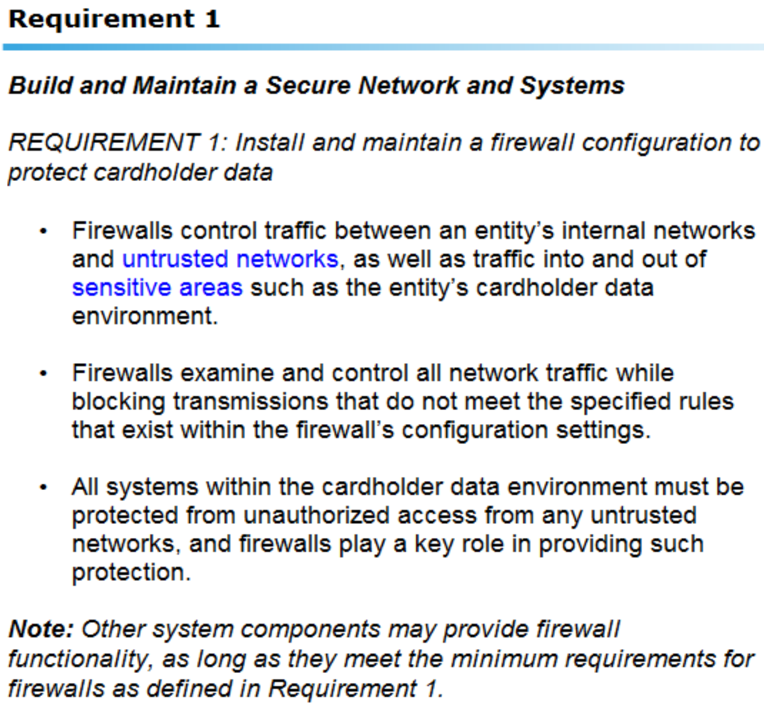
	Goals	PCI DSS Requirements
1	Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data
		2. Do not use vendor-supplied defaults for system passwords and other security parameters



Default password lists:

- http://www.phenoelit-us.org/
- http://www.cirt.net/passwords
- www.google.com
  - ➢ “default password”

PCI DSS – Build & Maintain a Secure Network



Requirement 1

Build and Maintain a Secure Network and Systems

REQUIREMENT 1: Install and maintain a firewall configuration to protect cardholder data

- Firewalls control traffic between an entity's internal networks and untrusted networks, as well as traffic into and out of sensitive areas such as the entity's cardholder data environment.

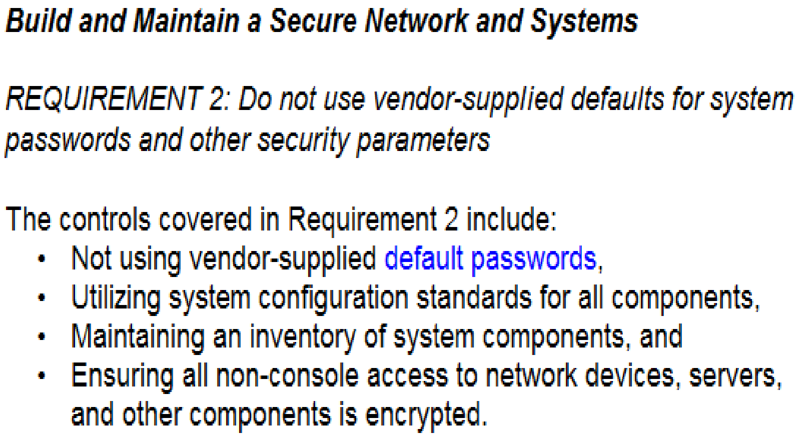
- Firewalls examine and control all network traffic while blocking transmissions that do not meet the specified rules that exist within the firewall's configuration settings.

- All systems within the cardholder data environment must be protected from unauthorized access from any untrusted networks, and firewalls play a key role in providing such protection.

Note: *Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in Requirement 1.*

PCI DSS – Build & Maintain a Secure Network

Requirement 2



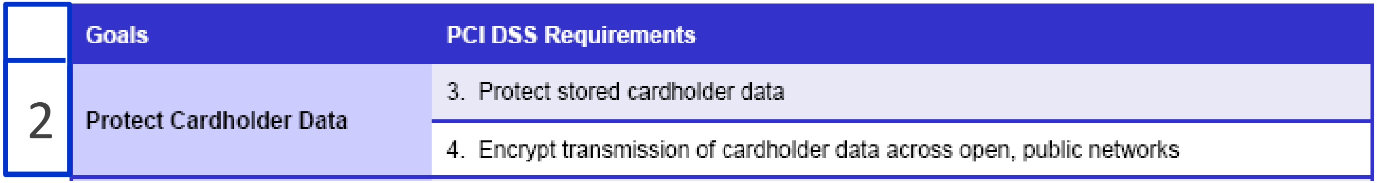
Build and Maintain a Secure Network and Systems

REQUIREMENT 2: Do not use vendor-supplied defaults for system passwords and other security parameters

The controls covered in Requirement 2 include:

- Not using vendor-supplied default passwords,
- Utilizing system configuration standards for all components,
- Maintaining an inventory of system components, and
- Ensuring all non-console access to network devices, servers, and other components is encrypted.

PCI DSS – Protect Cardholder Data



	Goals	PCI DSS Requirements
2	Protect Cardholder Data	3. Protect stored cardholder data
		4. Encrypt transmission of cardholder data across open, public networks

- Minimize storage
- Implement data retention and disposal policies
- Do NOT store sensitive authentication data
- Mask displayed PAN
- Render PAN unreadable where stored
- Protect cryptographic keys

➢ **ADDITION: NEVER send unprotected PAN by end user messaging (email, chat, IM, etc…)**

PCI DSS – Protect Cardholder Data

Requirement 3

Protect Cardholder Data

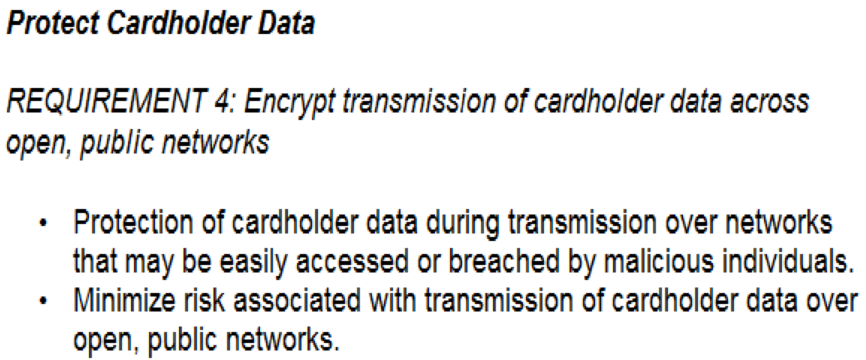
REQUIREMENT 3: Protect Stored Cardholder Data

- Protect stored data; specifically primary account numbers (PANs) and sensitive authentication data (SAD).
- Minimize risk associated with the storage of cardholder data.

If you don't need it, don't store it!

PCI DSS – Protect Cardholder Data

Requirement 4

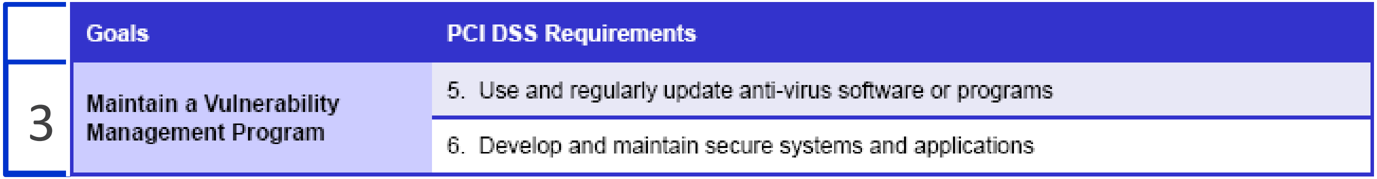


Protect Cardholder Data

REQUIREMENT 4: Encrypt transmission of cardholder data across open, public networks

- Protection of cardholder data during transmission over networks that may be easily accessed or breached by malicious individuals.
- Minimize risk associated with transmission of cardholder data over open, public networks.

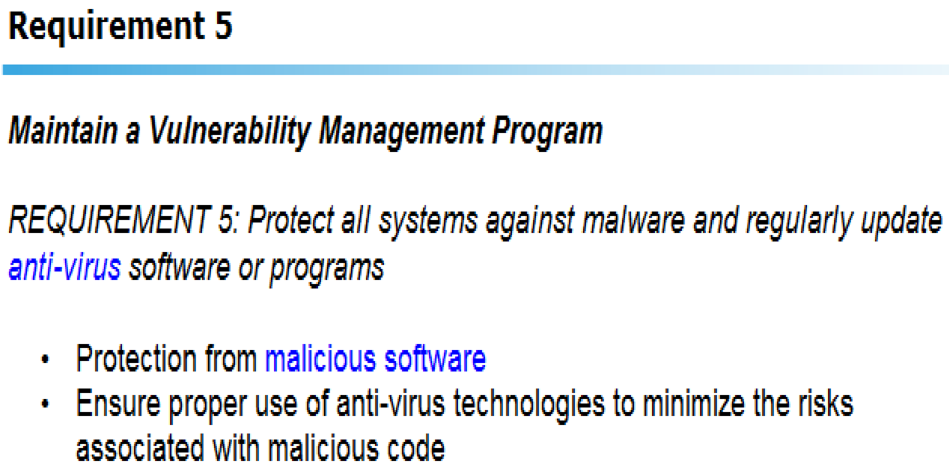
PCI DSS – Maintain Vulnerability Mgmt Program



	Goals	PCI DSS Requirements
3	Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs
		6. Develop and maintain secure systems and applications

- "Use anti-virus…"
- Secure software development and change control…
- Secure build checklists:
  - CIS offers vendor-neutral hardening resources
    http://www.cisecurity.org/
  - Microsoft Security Checklists
    http://www.microsoft.com/technet/archive/security/chklist/default.mspx?mfr=true
    http://technet.microsoft.com/en-us/library/dd366061.aspx
  - PA-DSS "certified" applications will have an Implementation Guide

PCI DSS – Maintain Vulnerability Mgmt Program



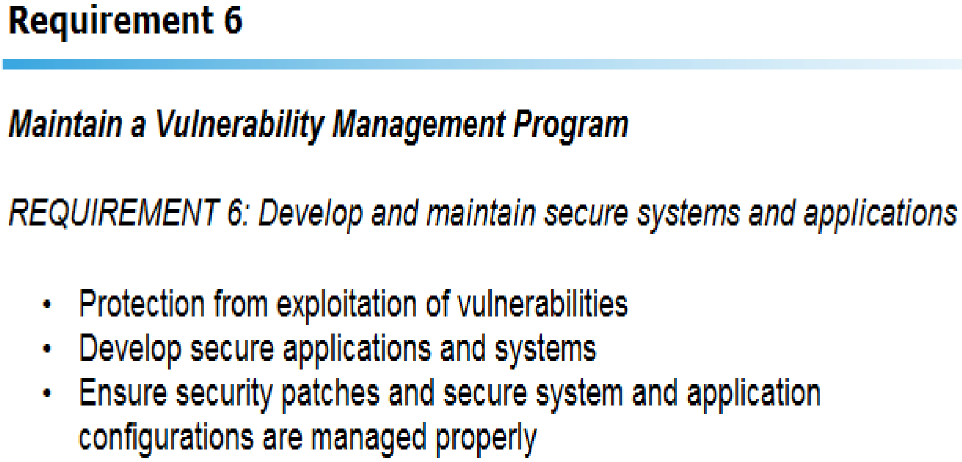
Requirement 5

Maintain a Vulnerability Management Program

REQUIREMENT 5: Protect all systems against malware and regularly update anti-virus software or programs

- Protection from malicious software
- Ensure proper use of anti-virus technologies to minimize the risks associated with malicious code

PCI DSS – Maintain Vulnerability Management Program



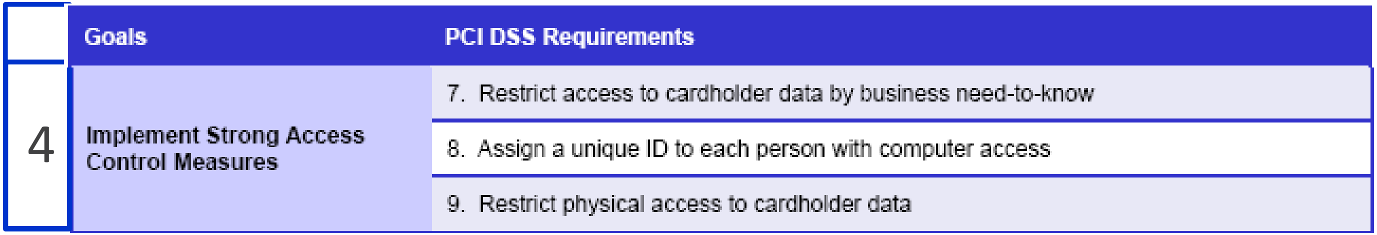
Requirement 6

Maintain a Vulnerability Management Program

REQUIREMENT 6: Develop and maintain secure systems and applications

- Protection from exploitation of vulnerabilities
- Develop secure applications and systems
- Ensure security patches and secure system and application configurations are managed properly

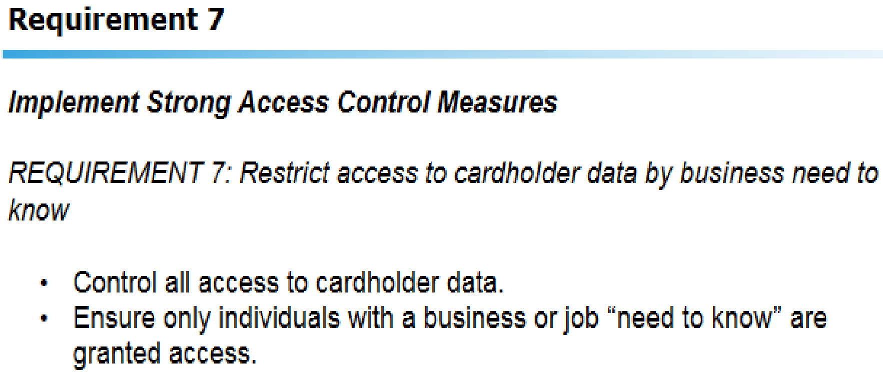
PCI DSS – Implement Strong Access Controls



	Goals	PCI DSS Requirements
4	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

- Principle of minimum access and least privilege
- Unique IDs (→ NO shared IDs)
- Long/strong passwords, password controls, strong authentication
- ➢ **Password protected screen saver time outs (15 min)**
- Limit and monitor physical access
- Secure storage and tracking of media

PCI DSS – Implement Strong Access Controls



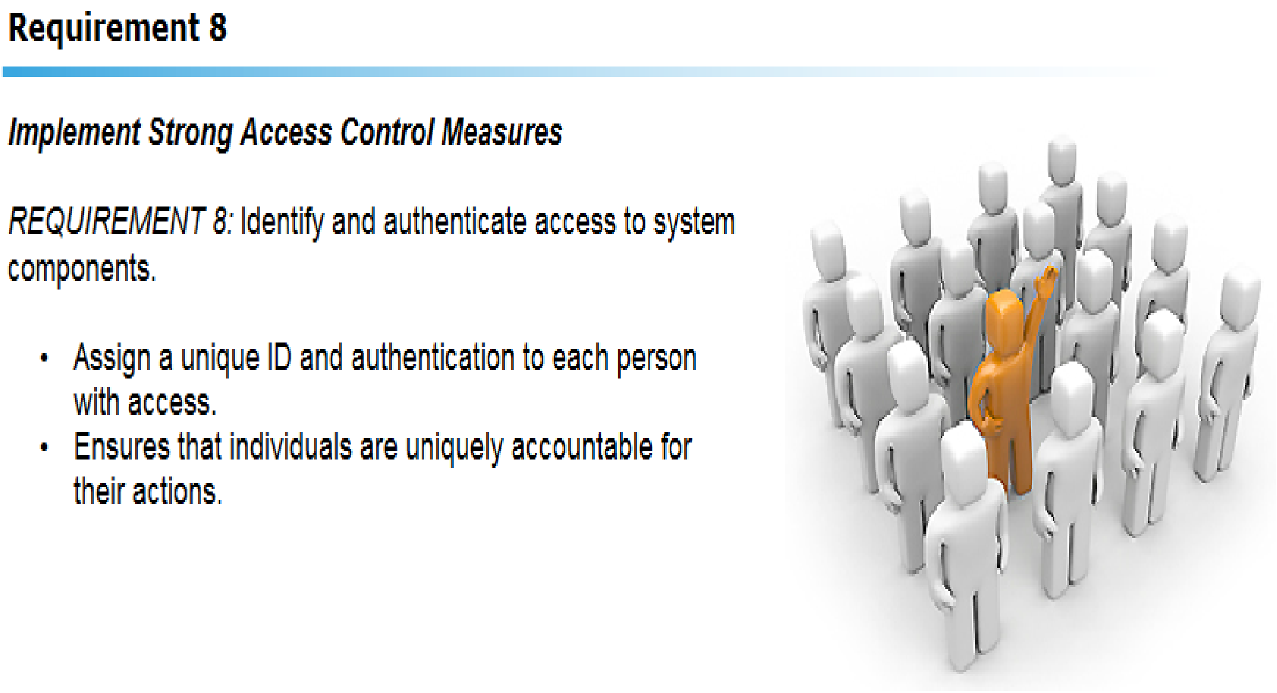
Requirement 7

Implement Strong Access Control Measures

REQUIREMENT 7: Restrict access to cardholder data by business need to know

- Control all access to cardholder data.
- Ensure only individuals with a business or job "need to know" are granted access.

PCI DSS – Implement Strong Access Controls



Requirement 8

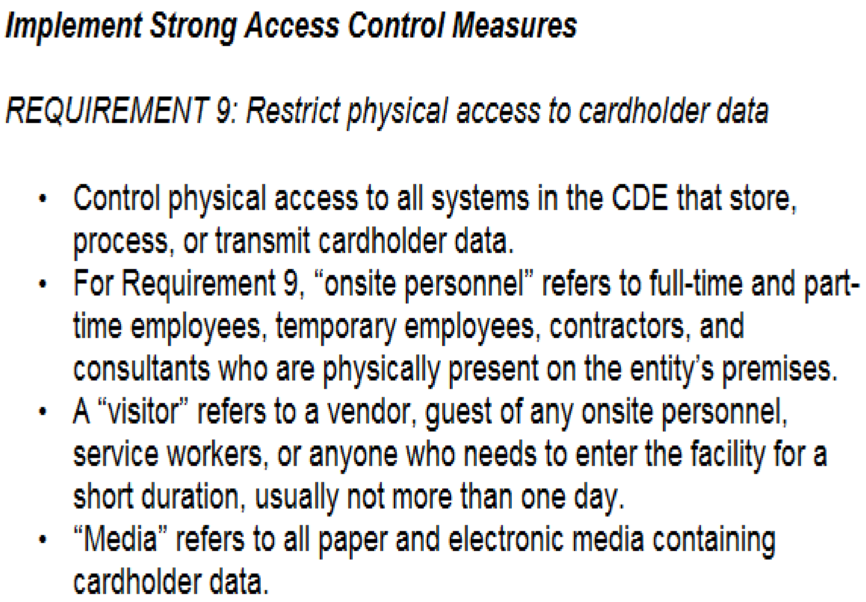
Implement Strong Access Control Measures

REQUIREMENT 8: Identify and authenticate access to system components.

- Assign a unique ID and authentication to each person with access.
- Ensures that individuals are uniquely accountable for their actions.

PCI DSS – Implement Strong Access Controls

Requirement 9

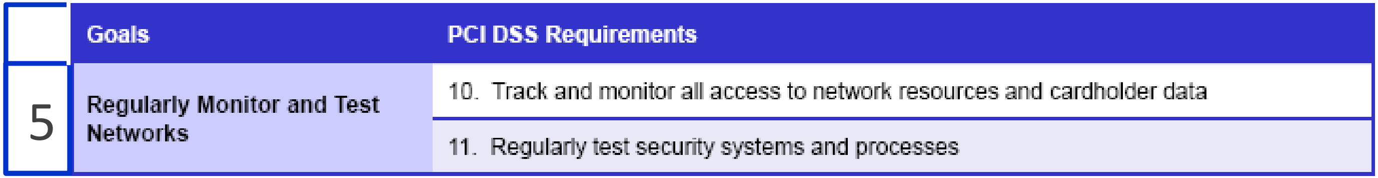


Implement Strong Access Control Measures

REQUIREMENT 9: Restrict physical access to cardholder data

- Control physical access to all systems in the CDE that store, process, or transmit cardholder data.
- For Requirement 9, “onsite personnel” refers to full-time and part-time employees, temporary employees, contractors, and consultants who are physically present on the entity’s premises.
- A “visitor” refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day.
- “Media” refers to all paper and electronic media containing cardholder data.

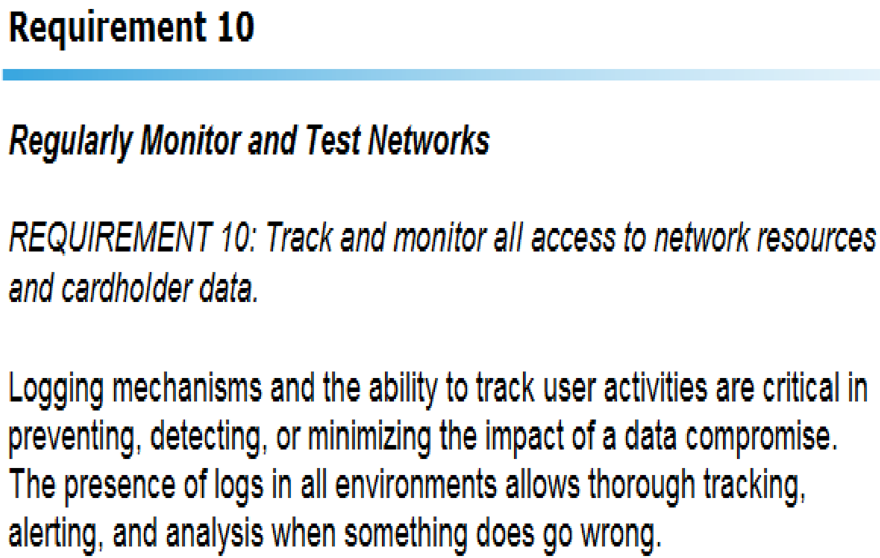
PCI DSS – Regularly Monitor and Test Networks



	Goals	PCI DSS Requirements
5	Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
		11. Regularly test security systems and processes

- Process, system, and application logging
- Secure the audit logs
- Review and retain audit logs
- Regular testing:
  - Quarterly*: Wireless testing & Vulnerability scanning
  - Annual*: Penetration testing
- IDS/IPS and
- File integrity monitoring

PCI DSS – Regularly Monitor and Test Networks



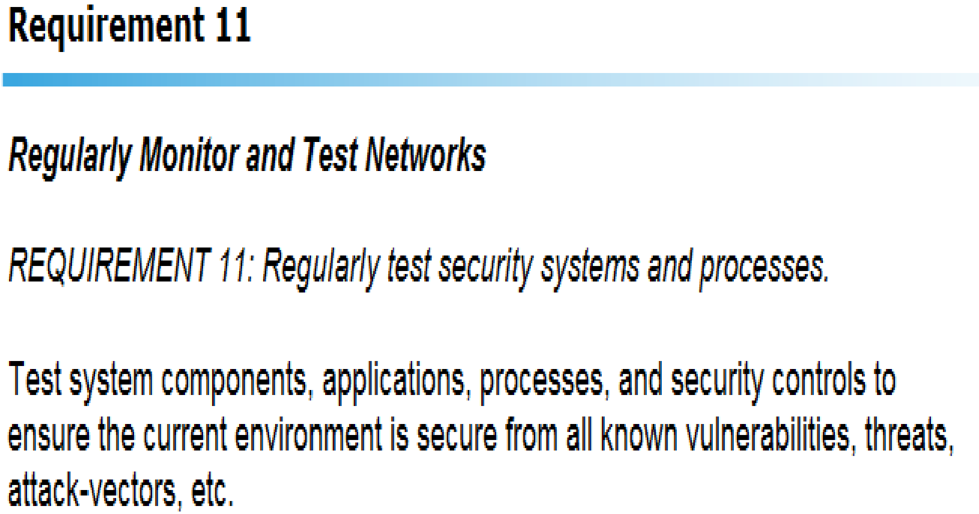
Requirement 10

Regularly Monitor and Test Networks

REQUIREMENT 10: Track and monitor all access to network resources and cardholder data.

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong.

PCI DSS – Regularly Monitor and Test Networks



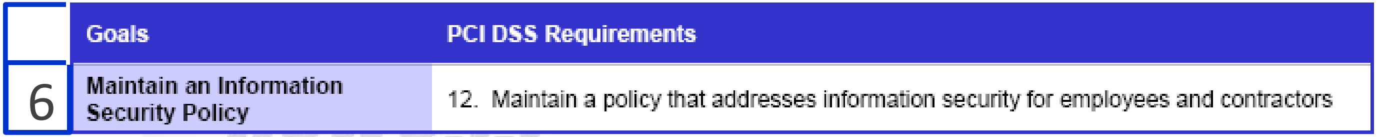
Requirement 11

Regularly Monitor and Test Networks

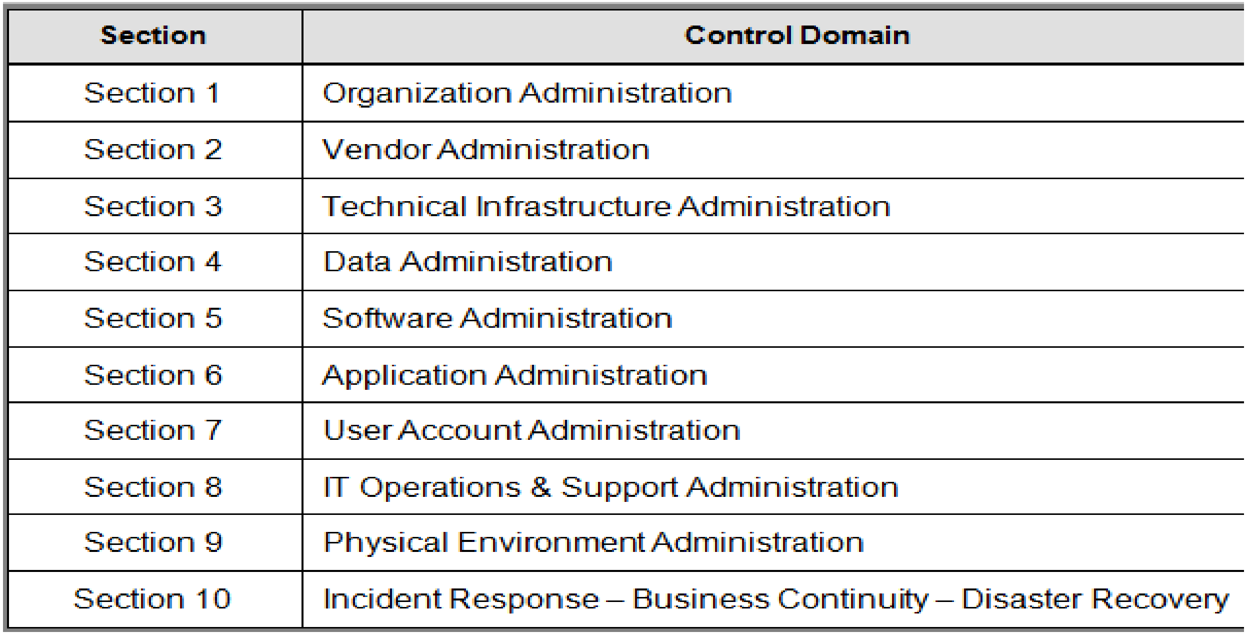
REQUIREMENT 11: Regularly test security systems and processes.

Test system components, applications, processes, and security controls to ensure the current environment is secure from all known vulnerabilities, threats, attack-vectors, etc.

PCI DSS – Maintain Information Security Policy



	Goals	PCI DSS Requirements
6	Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors



Section	Control Domain
Section 1	Organization Administration
Section 2	Vendor Administration
Section 3	Technical Infrastructure Administration
Section 4	Data Administration
Section 5	Software Administration
Section 6	Application Administration
Section 7	User Account Administration
Section 8	IT Operations & Support Administration
Section 9	Physical Environment Administration
Section 10	Incident Response – Business Continuity – Disaster Recovery

DSS 3.2 to DSS 3.2.1 Highlighted Changes

- Addressed minor punctuation and format issues.
- SSL/early TLS migration effort, as the migration date of July 1, 2018 has passed.

- PCI DSS continues to be updated to be relevant to known risks.
  - PCI Software Security Framework (PCI SSF)

How PCI Relates to Credit Unions

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

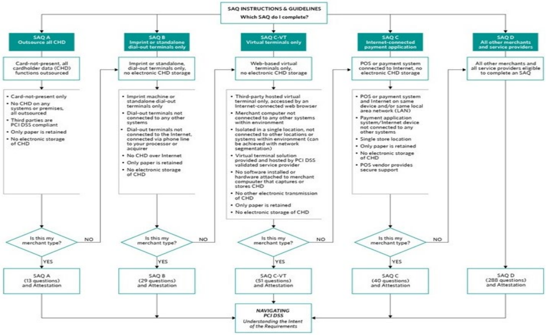
Investment advisory services are offered through CliftonLarsonAllen Wealth Advisors, LLC, an SEC-registered investment advisor

Exercise

- Think about how your credit union stores, processes, or transmits credit card information
- Think in terms of the steps/stages followed
  - Examples:
    - ◊ Accept payment information over the phone
    - ◊ Members make payments online
    - ◊ Receive payment information in the mail
    - ◊ Member statements are sent/stored/reviewed by member services reps
- End Goal is to understand “where the card data lives”

Understand Where Your Data Lives

- Develop data inventory
  - Payment/data flow
  - Where static data resides



SAQ INSTRUCTIONS & GUIDELINES
Which SAQ do I complete?

SAQ A
Outsource all CHD

Card-not-present, all cardholder data (CHD) functions outsourced

- Card-not-present only
- No CHD on any systems or premises, all outsourced
- Third parties are PCI DSS compliant
- Only paper is retained
- No electronic storage of CHD

SAQ A
(13 questions)
and Attestation

SAQ B
Imprint or standalone dial-out terminals only

Imprint or standalone, dial-out terminals only, no electronic CHD storage

- Imprint machine or standalone dial-out terminals only
- Dial-out terminals not connected to any other systems
- Dial-out terminals not connected to the Internet, connected via phone line to your processor or acquirer
- No CHD over Internet
- Only paper is retained
- No electronic storage of CHD

SAQ B
(29 questions)
and Attestation

SAQ C-VT
Virtual terminals only

Web-based virtual terminals only, no electronic CHD storage

- Third-party hosted virtual terminal only, accessed by an Internet-connected web browser
- Merchant computer not connected to any other systems within environment
- Isolated in a single location, not connected to other locations or systems within environment (can be achieved with network segmentation)
- Virtual terminal solution provided and hosted by PCI DSS validated service provider
- No software installed or hardware attached to merchant compuuter that captures or stores CHD
- No other electronic transmission of CHD
- Only paper is retained
- No electronic storage of CHD

SAQ C-VT
(51 questions)
and Attestation

SAQ C
Internet-connected payment application

POS or payment system connected to Internet, no electronic CHD storage

- POS or payment system and Internet on same device and/or same local area network (LAN)
- Payment application system/Internet device not connected to any other systems
- Single store location
- Only paper is retained
- No electronic storage of CHD
- POS vendor provides secure support

SAQ C
(40 questions)
and Attestation

SAQ D
All other merchants and service providers

All other merchants and all service providers eligible to complete an SAQ

SAQ D
(288 questions)
and Attestation

NAVIGATING PCI DSS
Understanding the Intent of the Requirements

- Who is mining data and for what purposes
- Understand how the back up system works

Exercise (repeat…)

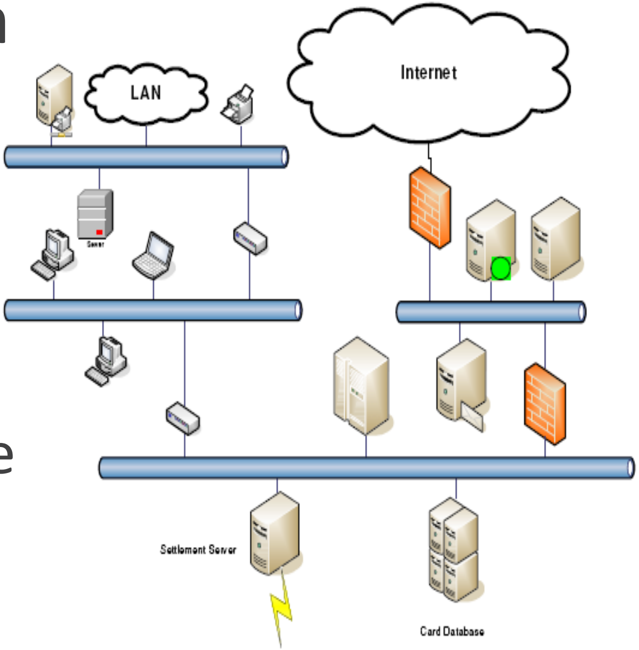
- Do you accept CC payment “in-person”?
- Do you accept CC payment over the phone?
- Do you accept CC payment via a website?
- Do you rely on a 3rd party/vendor to host or manage any of your data systems?
- Do you store or process CC data for someone else?
- Do you have instant issue capabilities?
- Are ATMs “on your network”?

Most Significant Challenges to PCI Compliance?

7. Identify where card holder data is “stored”
6. Compare current control requirements to PCI – identify overlaps and gaps
5. Secure application development/compliance
4. Vulnerability management and remediation
3. Secure standard configuration management
2. Network segmentation
1. Operational maturity:
    - Disciplined adherence to policies and procedures
    - Mature documented exception management process

Common Struggles for Credit Unions

- Isolation/segmentation is difficult
  - Everything talks with the core
  - This makes all systems on the network in scope

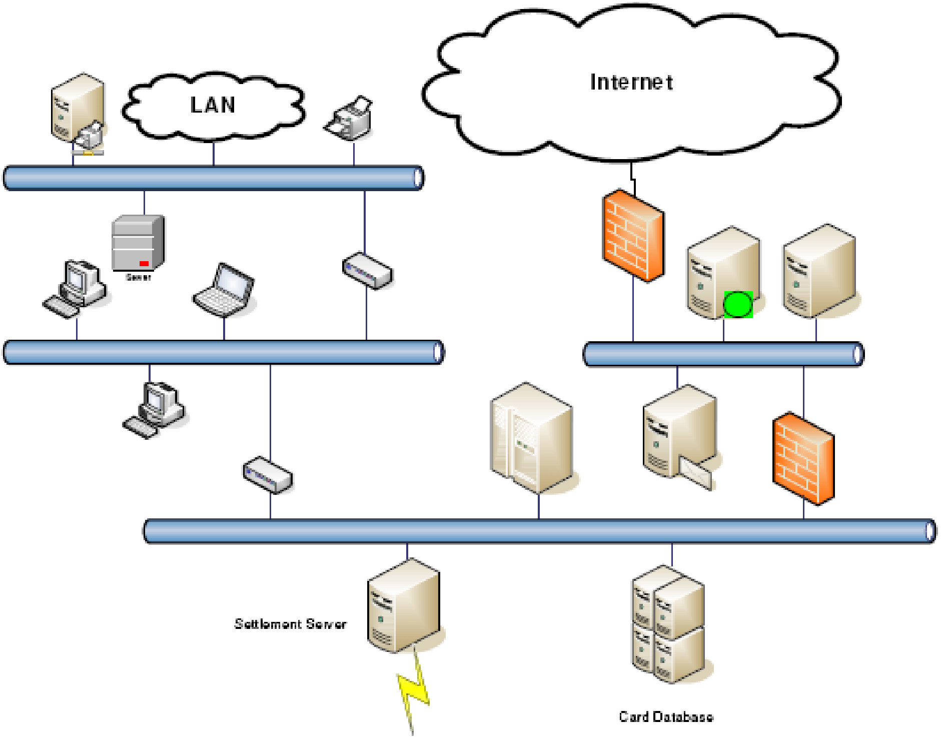


Exercise - Segment Your Network

- What is in-scope here?

➢ NOTHING
➢ Firewalls
➢ Servers
➢ PCs
➢ Everything

- Why?

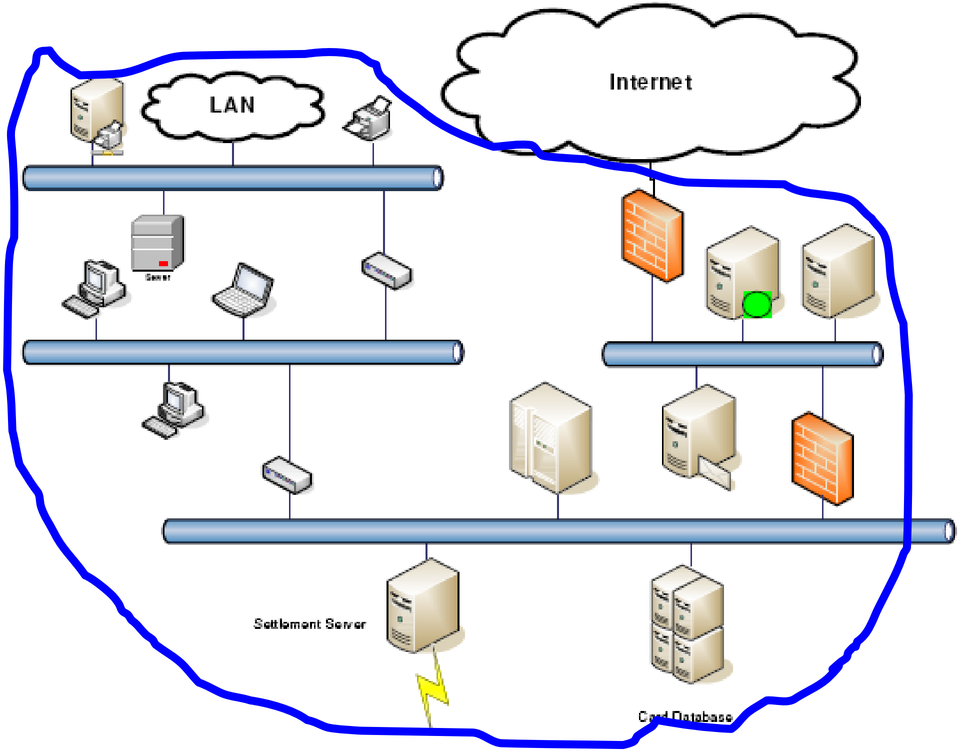


Exercise - Segment Your Network

- What is in-scope here?

- ➢ NOTHING
- ➢ Firewalls
- ➢ Servers
- ➢ PCs
- ➢ Everything

- Why?

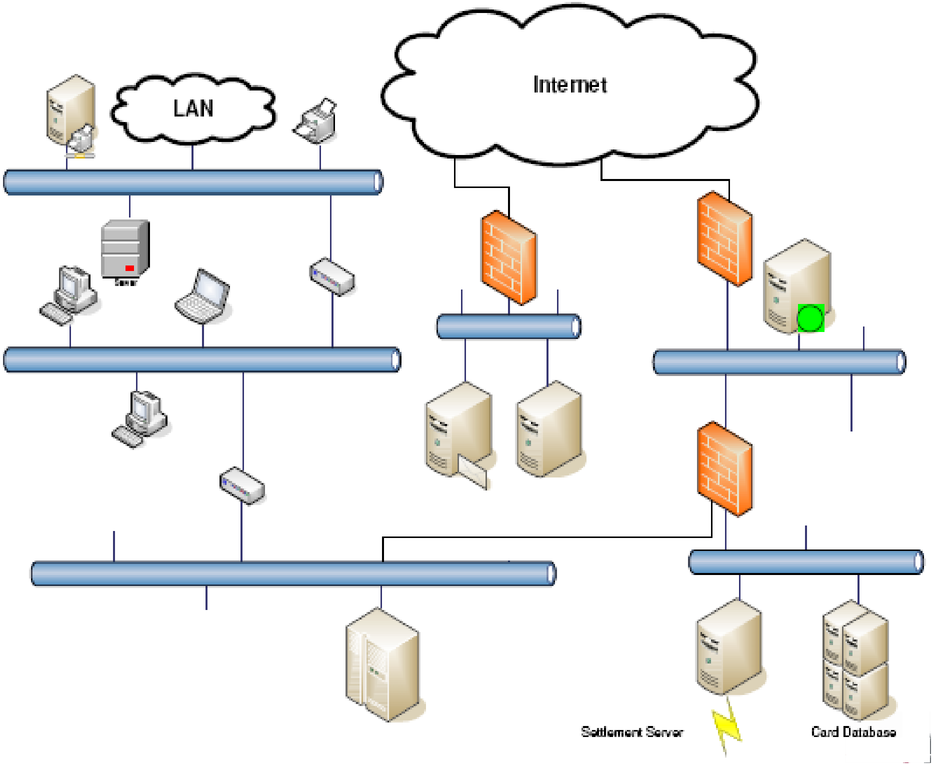


Segment Your Network

What is in-scope here?

- ➢NOTHING
- ➢Firewalls
- ➢Servers
- ➢PCs
- ➢Everything

Why?

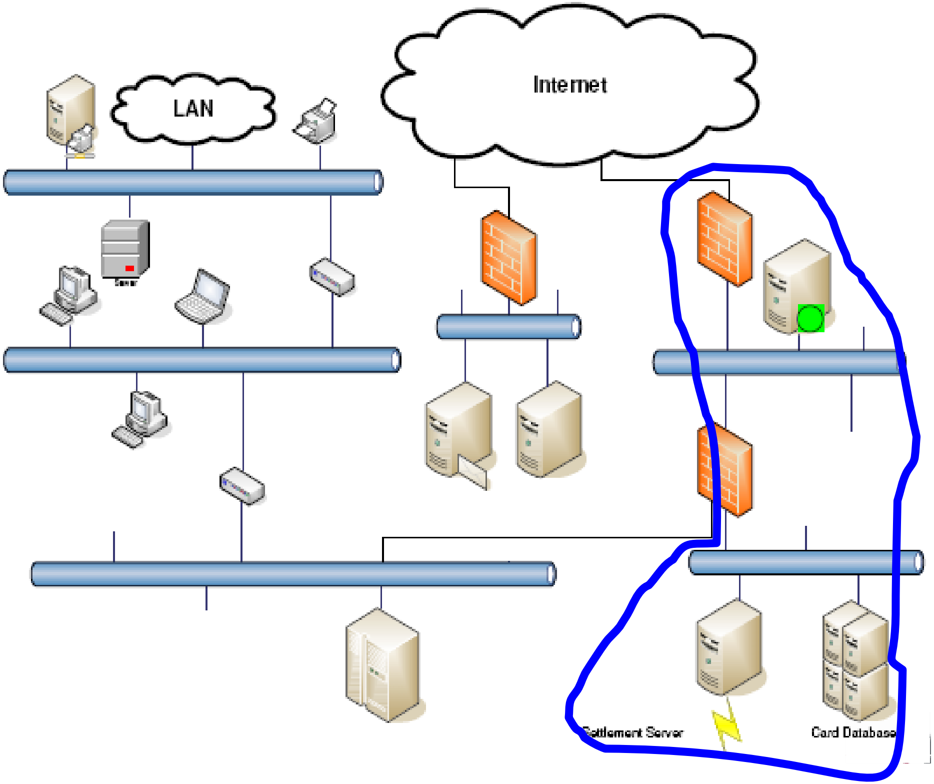


Segment Your Network

What is in-scope here?

- ➢NOTHING
- ➢Firewalls
- ➢Servers
- ➢PCs
- ➢Everything

Why?



Common Struggles for Credit Unions

- Reports (PDF, XLSX, etc.) contain PAN
  - Core/vendor software generates reports with PAN data
  - These reports exist in email and on network file shares
- Data warehouse and analytics…

Common Struggles for Credit Unions

- Card data is received over the phone
  - Service center records phone calls
  - Phone calls contain PAN data

Common Struggles for Credit Unions

- Vendor software doesn’t follow PCI guidelines
  - Instant issue systems store SAD
  - Vendor software stores clear-text PAN
  - Etc.

Common Struggles for Credit Unions

- Members have old systems
  - Credit Union wants to support legacy (non-compliant) protocols for members with old PCs

Summarize

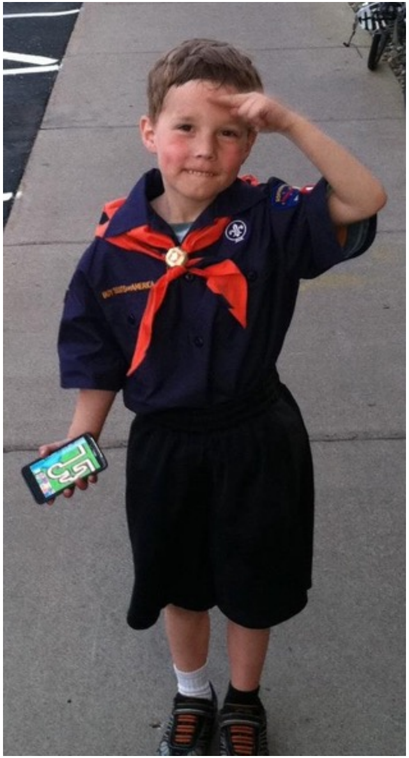
1. Credit unions need to be PCI compliant
2. There is no “PCI Police” looking for you
3. Some examiners are starting to ask about compliance status
4. Most Credit Unions are both Merchants and Service Providers
   - Could be Level 1 or Level 2 service provider

Summarize

5. You need to complete SAQ-D
   - All 400+ controls are in scope and need to be reviewed
6. You most likely are not compliant right now
7. Start the process to self-assess your own compliance status

Summarize

8. Where to start?
   - Identify where card data lives and how it flows through environment
   - Update policies and processes to address PCI requirements
   - Follow PCI Prioritized Approach



Questions?

CLAconnect.com

“Information technology and business are becoming inextricably interwoven. I don’t think anybody can talk meaningfully about one without talking about the other.”
-Bill Gates

Randy Romes, CISSP, CRISC, CISA, MCP, PCI-QSA
Managing Principal – Cybersecurity Services Team

randy.romes@CLAconnect.com
612.397.3114 – office
612.554.3967 - cell