MNP
Cyber Security

PCI Training

PCI & You: more than you wanted to know.

Presented by: Jason Murray

Date: February 1, 2017

pci
Security
Standards Council
TM

Payment Card Industry Security Standards

- Many Different Forms of Payment
  - Pay Now
  - Pay Later
  - Pay in Advance
- Many Different Security Standards
  - PCI DSS
  - EMV 4.1, CPA 1.0, CPS, etc.
  - Chip and Pin, Link
  - PA-DSS
  - PTS
  - P2PE
  - ASV
  - QIR
  - PFI
- Which Applies?
- Compliance with one standard is not automatic compliance with another

PCI Ecosystem

The Council

PCI Security Standards Council

- Qualified Security Assessor (QSA)
- Payment Application QSA (PA-QSA)
- P2PE QSA
- Approved Scanning Vendor (ASV)
- Internal Security Assessor (ISA)
- PCI Forensic Investigator (QFI)
- Qualified Integrator and Reseller (QIR)
- PCI Professional (PCIP)

PCI Ecosystem

The Card Brands

- MasterCard (MC)
  - Site Data Protection
  - Incident Response & Forensics
  - PIN Security Auditor
  - Service Provider Registry

- VISA
  - Incident Response & Forensics
  - Forensics Standard
  - VISA PIN-Security Auditor
  - Provide Quantitative Risk Metrics to Visa

- Discover Financial
  - First Responders Training Program
  - Incident Response & Forensics Provider

- American Express (AMEX)
  - Incident Response & Forensics Provider

- Japan Credit Bank (JCB)
  - Incident Response & Forensics Provider

PCI Ecosystem

The Banks

- Issuing Banks
  - Issues cards to consumers
  - Extends a line of credit to card holders
  - Assumes primary liability for consumers' in-ability to pay

Moneris
SOLUTIONS

- Acquiring Banks
  - Accepts card transactions on behalf of the merchant
  - Extends a line of credit to the merchant
  - Exchanges funds with issuing banks on merchant's behalf

3rd Party Agent

- Member Service Provider
- Independent Sales Organization
- VISA Net
  - Handle CHD on behalf of the merchant
  - Provide payment services

- Merchant Service Provider
  - Not directly in the payment channel
  - Provides other kinds of support to merchants

PCI Ecosystem

The Merchants (You)

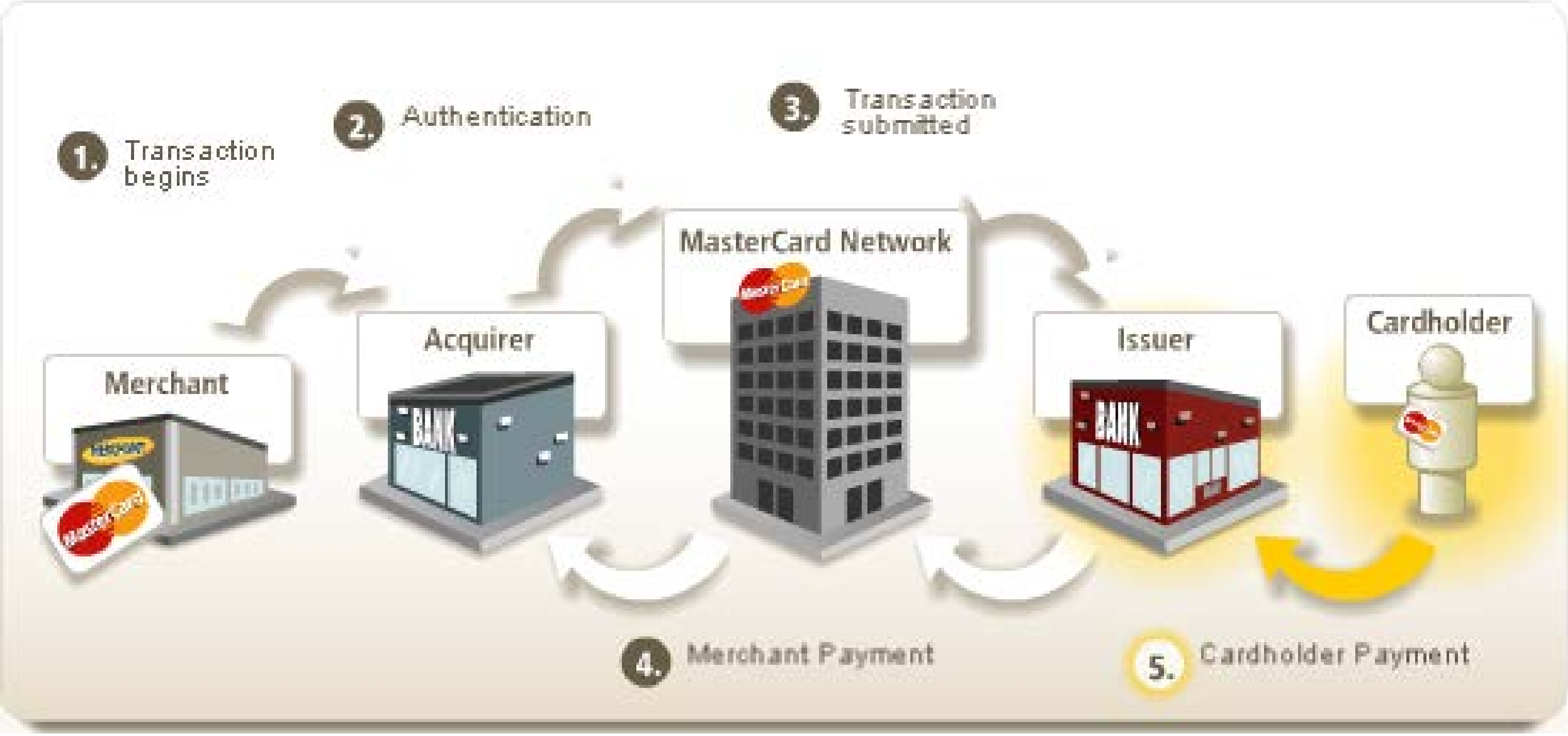
PCI Ecosystem

The Cardholder (Customers)

Anatomy of a Card Transaction

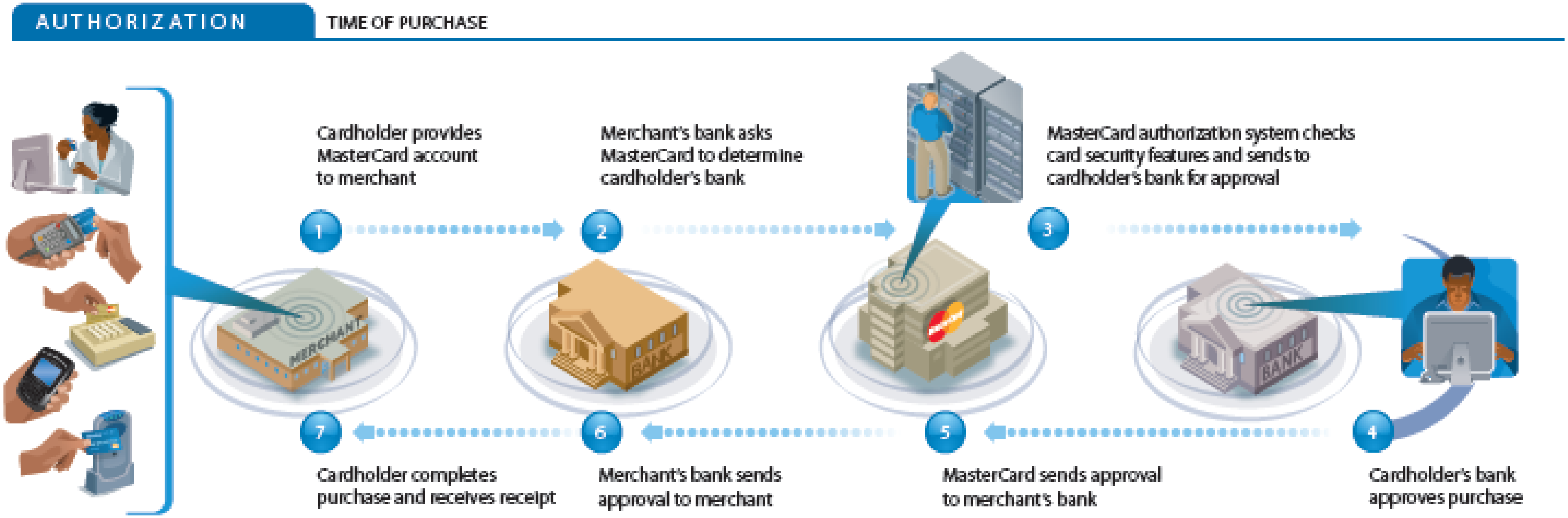
Follow the Money.

Anatomy of a Card Transaction



Source: MasterCard Worldwide

Anatomy of a Card Transaction - Authorisation



AUTHORIZATION

TIME OF PURCHASE

1 Cardholder provides MasterCard account to merchant

2 Merchant's bank asks MasterCard to determine cardholder's bank

3 MasterCard authorization system checks card security features and sends to cardholder's bank for approval

4 Cardholder's bank approves purchase

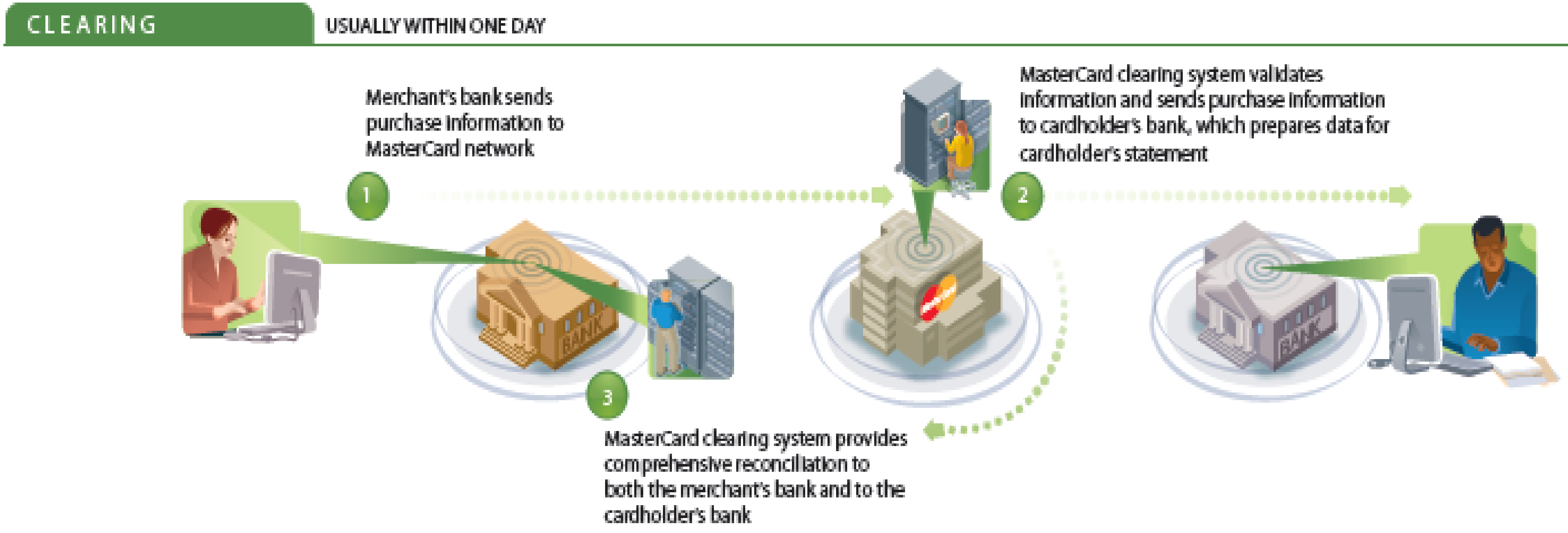
5 MasterCard sends approval to merchant's bank

6 Merchant's bank sends approval to merchant

7 Cardholder completes purchase and receives receipt

Source: MasterCard Worldwide

Anatomy of a Card Transaction - Clearing



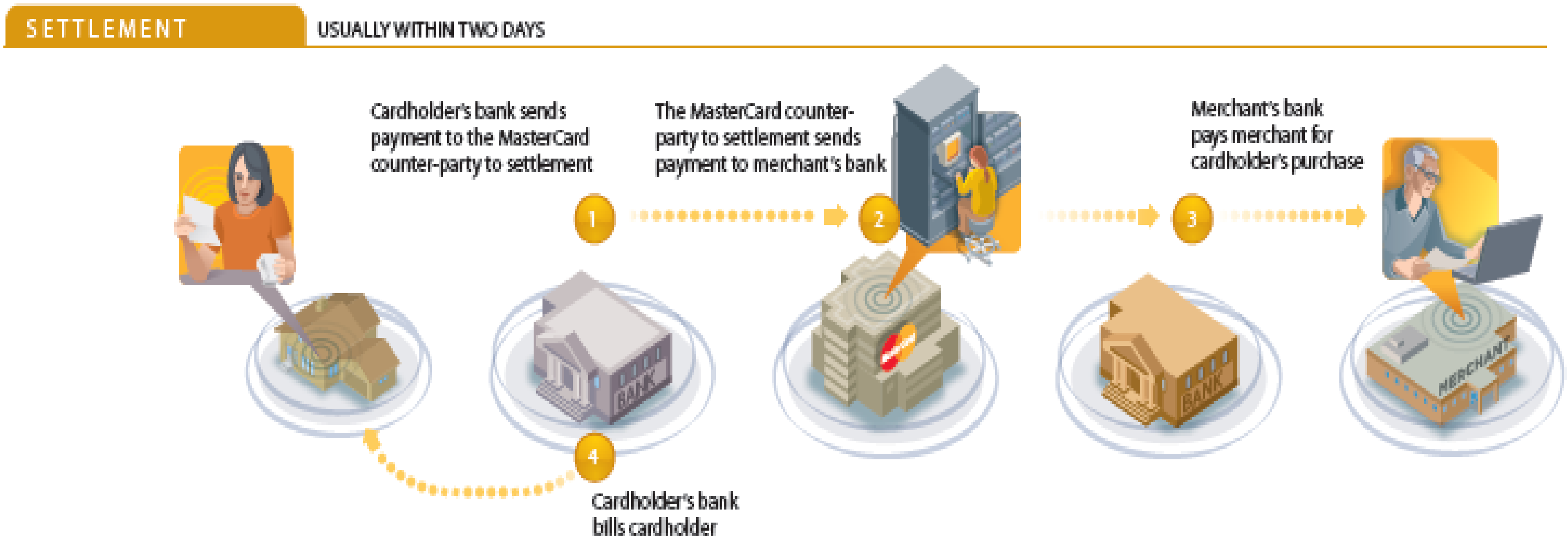
1 Merchant's bank sends purchase information to MasterCard network

2 MasterCard clearing system validates information and sends purchase information to cardholder's bank, which prepares data for cardholder's statement

3 MasterCard clearing system provides comprehensive reconciliation to both the merchant's bank and to the cardholder's bank

Source: MasterCard Worldwide

Anatomy of a Card Transaction - Settlement



SETTLEMENT USUALLY WITHIN TWO DAYS

1 Cardholder's bank sends payment to the MasterCard counter-party to settlement

2 The MasterCard counter-party to settlement sends payment to merchant's bank

3 Merchant's bank pays merchant for cardholder's purchase

4 Cardholder's bank bills cardholder

Source: MasterCard Worldwide

Anatomy of a Credit Card

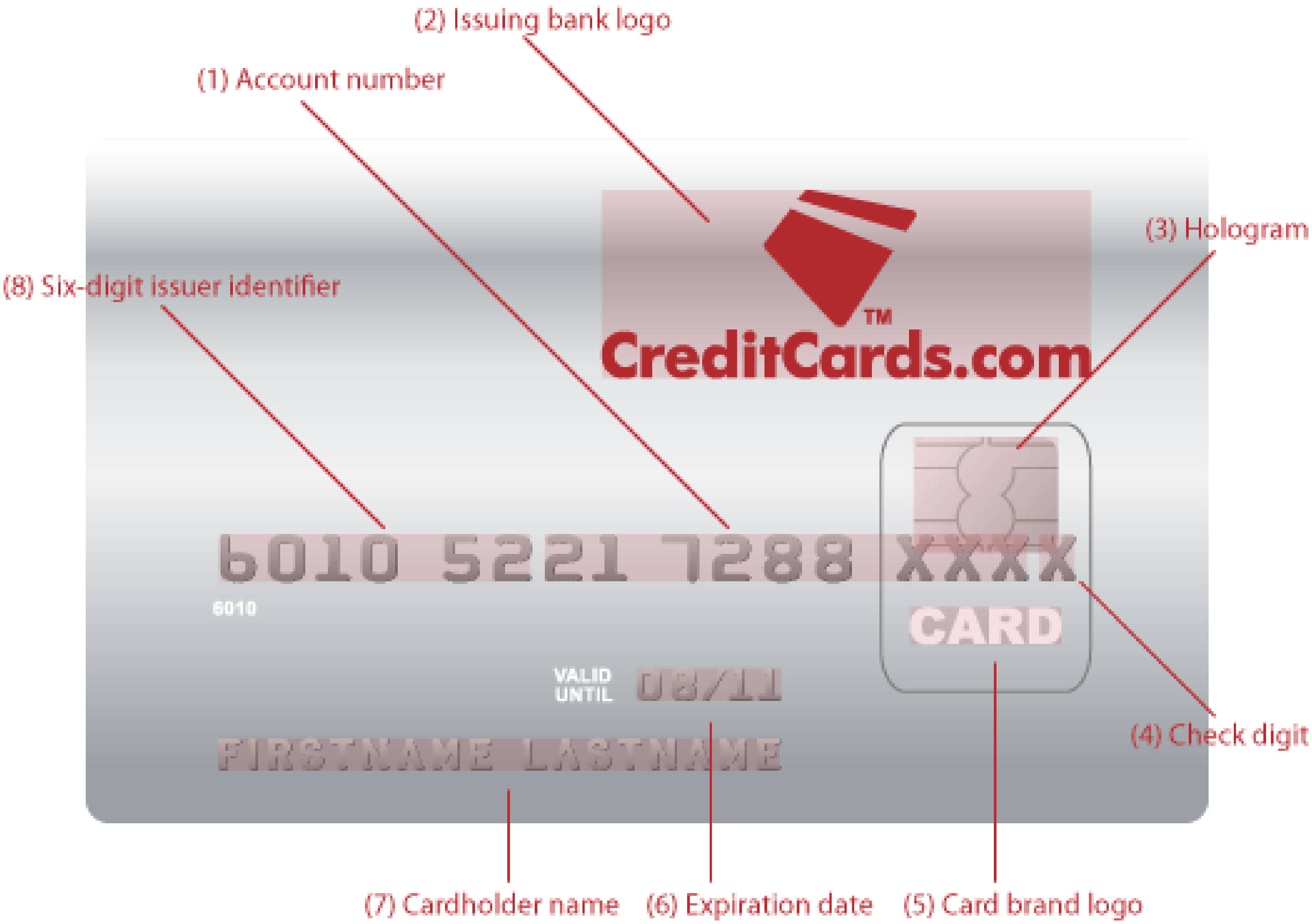
Charge It!

The Anatomy of a Credit Card

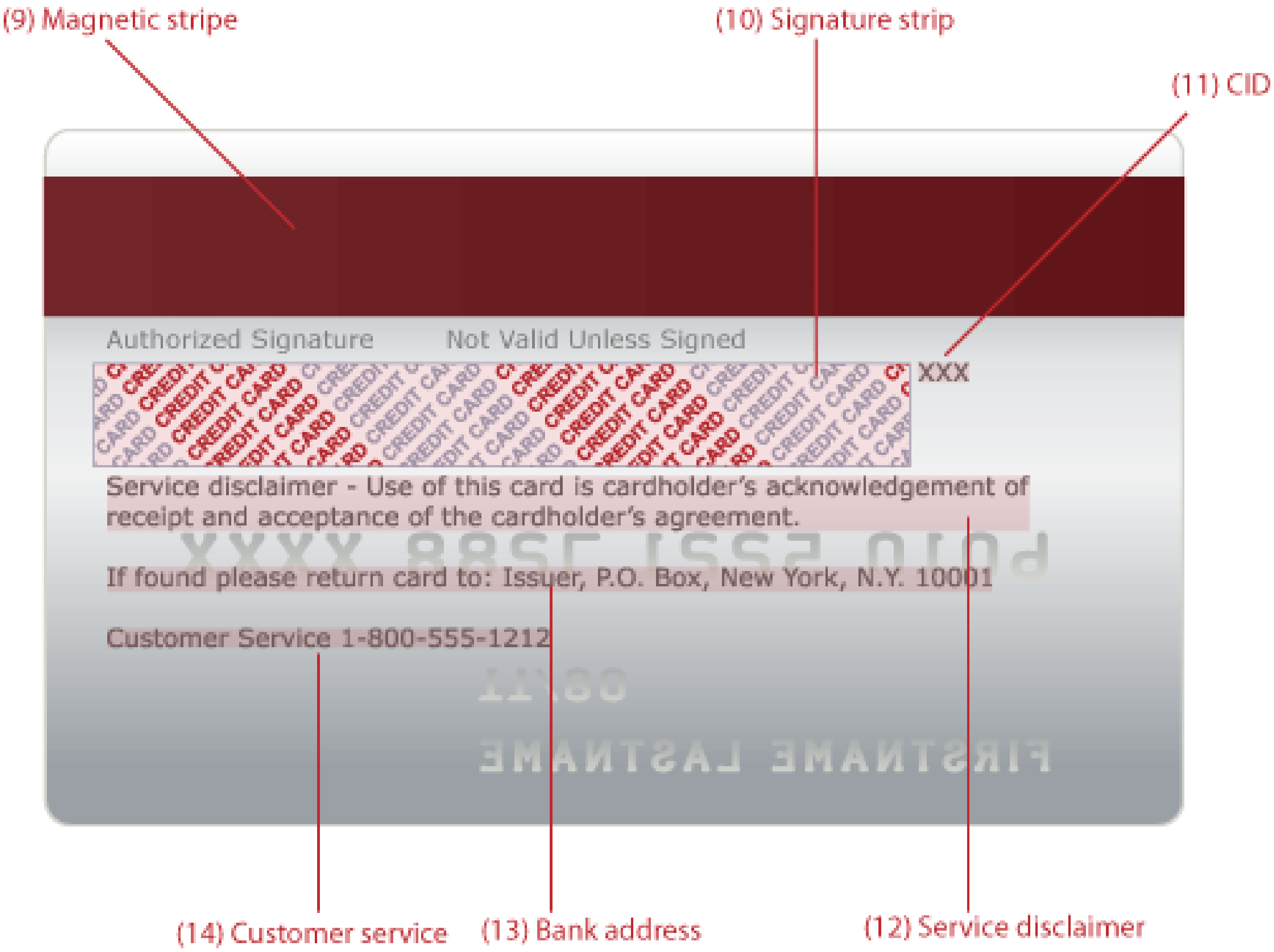
Cardholder data is defined as the primary account number ("PAN," or credit card number) and other data obtained as part of a payment transaction, including the following data elements:

- PAN
- Cardholder Name
- Expiration Date
- Service Code
- Sensitive Authentication Data:
  - full magnetic stripe data
  - CAV2/CVC2/CVV2/CID
  - PINs/PIN blocks

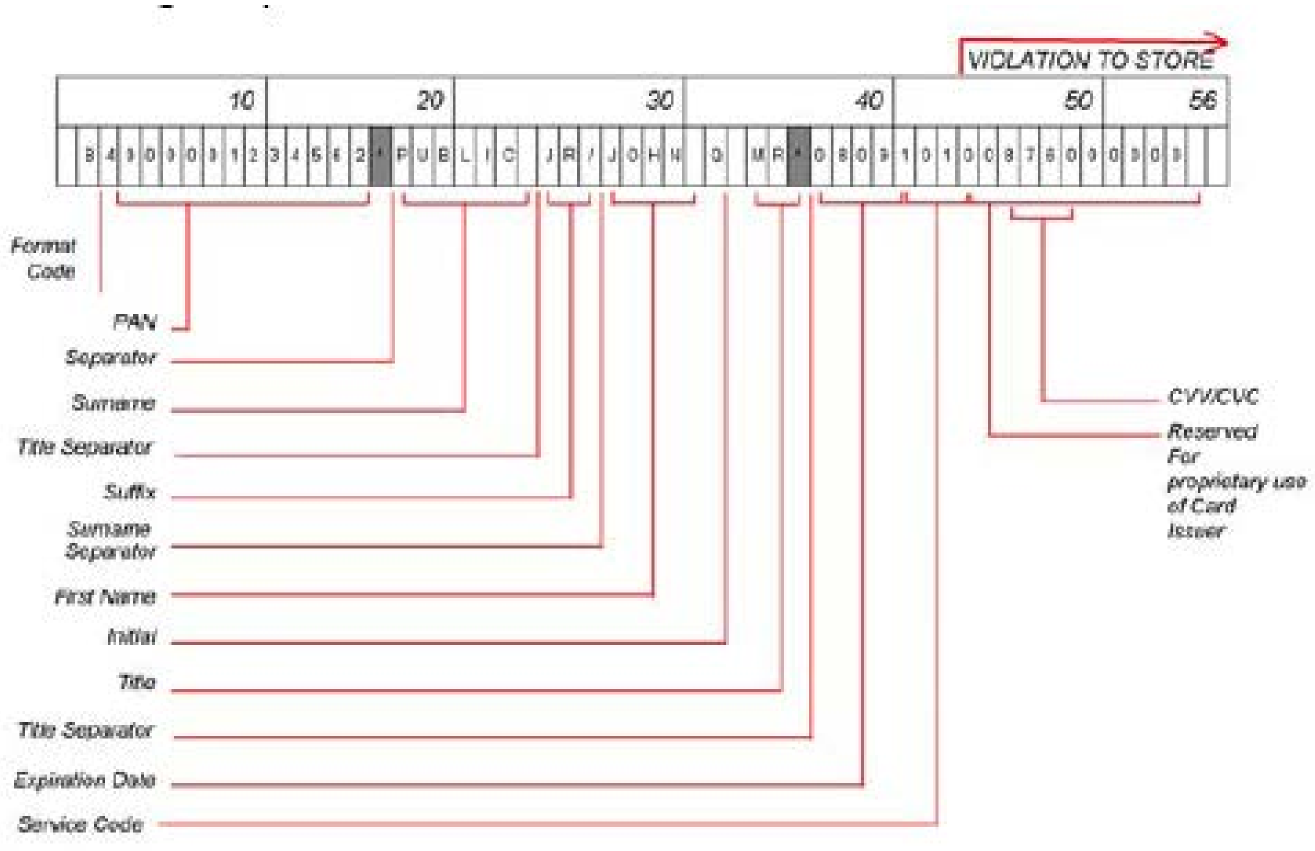
The Anatomy of a Credit Card (Front)



The Anatomy of a Credit Card (Back)


(9) Magnetic stripe
(10) Signature strip
(11) CID
Authorized Signature
Not Valid Unless Signed
XXX
Service disclaimer - Use of this card is cardholder's acknowledgement of receipt and acceptance of the cardholder's agreement.
If found please return card to: Issuer, P.O. Box, New York, N.Y. 10001
Customer Service 1-800-555-1212
(14) Customer service
(13) Bank address
(12) Service disclaimer

The Anatomy of a Credit Card (Cont.)

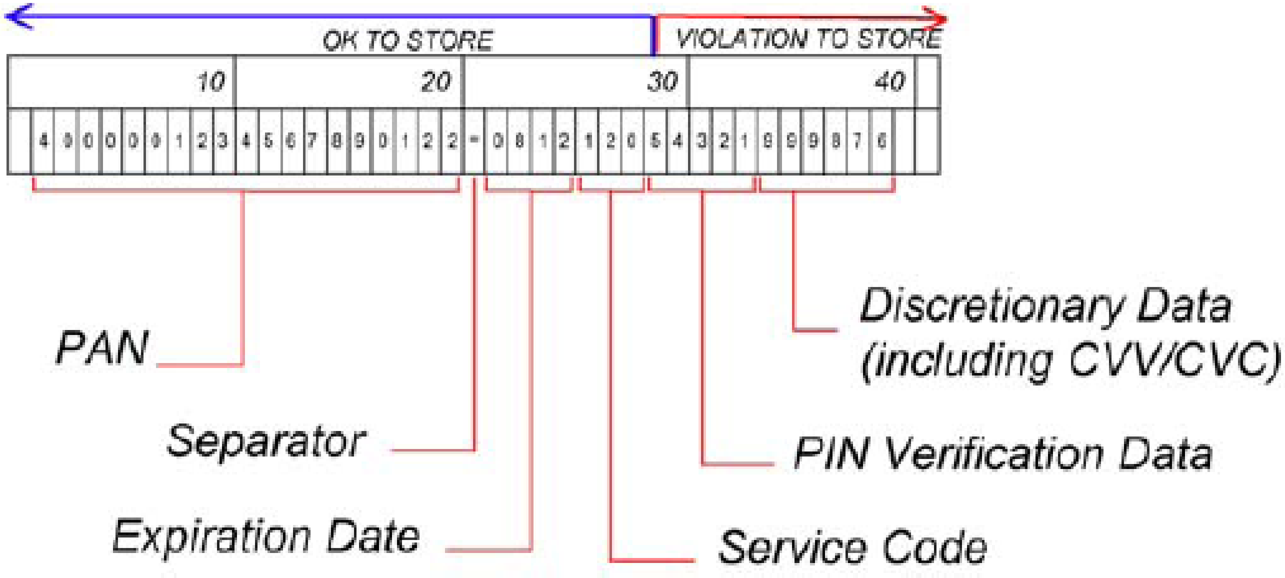


Source: PCI Secure Standard Council

Track 1

- Contains all fields of both track 1 and track 2
- Length up to 79 characters

The Anatomy of a Credit Card (Cont.)

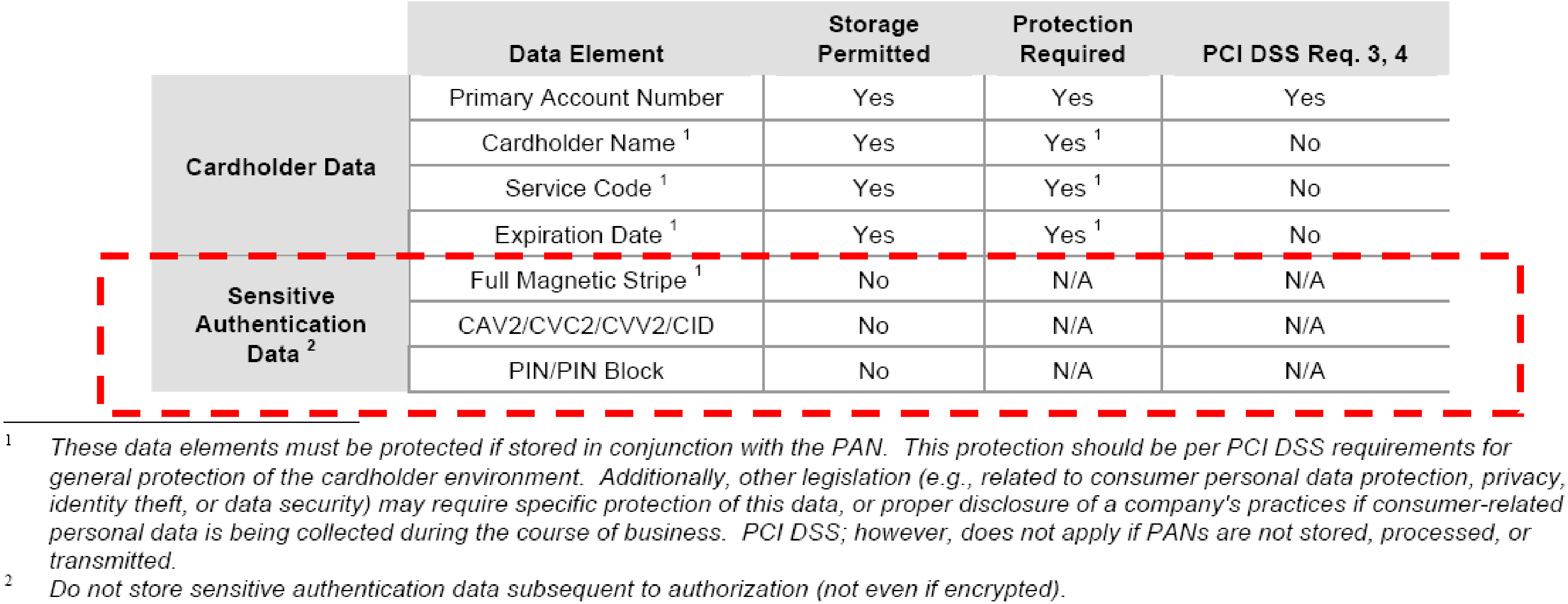


Track 2

- Shorter processing time for older dial-up transmissions
- Length up to 40 characters

Source: PCI Secure Standard Council

The Anatomy of a Credit Card (Cont.)



	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3, 4
Cardholder Data	Primary Account Number	Yes	Yes	Yes
	Cardholder Name [1]	Yes	Yes [1]	No
	Service Code [1]	Yes	Yes [1]	No
	Expiration Date [1]	Yes	Yes [1]	No
Sensitive Authentication Data [2]	Full Magnetic Stripe [1]	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

[1] *These data elements must be protected if stored in conjunction with the PAN. This protection should be per PCI DSS requirements for general protection of the cardholder environment. Additionally, other legislation (e.g., related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data, or proper disclosure of a company's practices if consumer-related personal data is being collected during the course of business. PCI DSS; however, does not apply if PANs are not stored, processed, or transmitted.*

[2] *Do not store sensitive authentication data subsequent to authorization (not even if encrypted).*

Source: PCI Secure Standard Council

PCI Compliance

Not just “the law,” a good idea.

Compliance vs Validation

Who Must Comply?

Anyone who:

- – Accepts,
- – Processes,
- – Stores,
- – Transmits, or
- – Can affect the security of Cardholder Data (CHD)

Why Is Compliance Important? - Fines

- It is important to be familiar with the applicable merchant account agreement, which should outline your exposure.
- The following table is an example of a time-cost schedule which Visa uses.

Month	How much
1 to 3	$10,000 monthly
4 to 6	$50,000 monthly
7 and on	$100,000 monthly

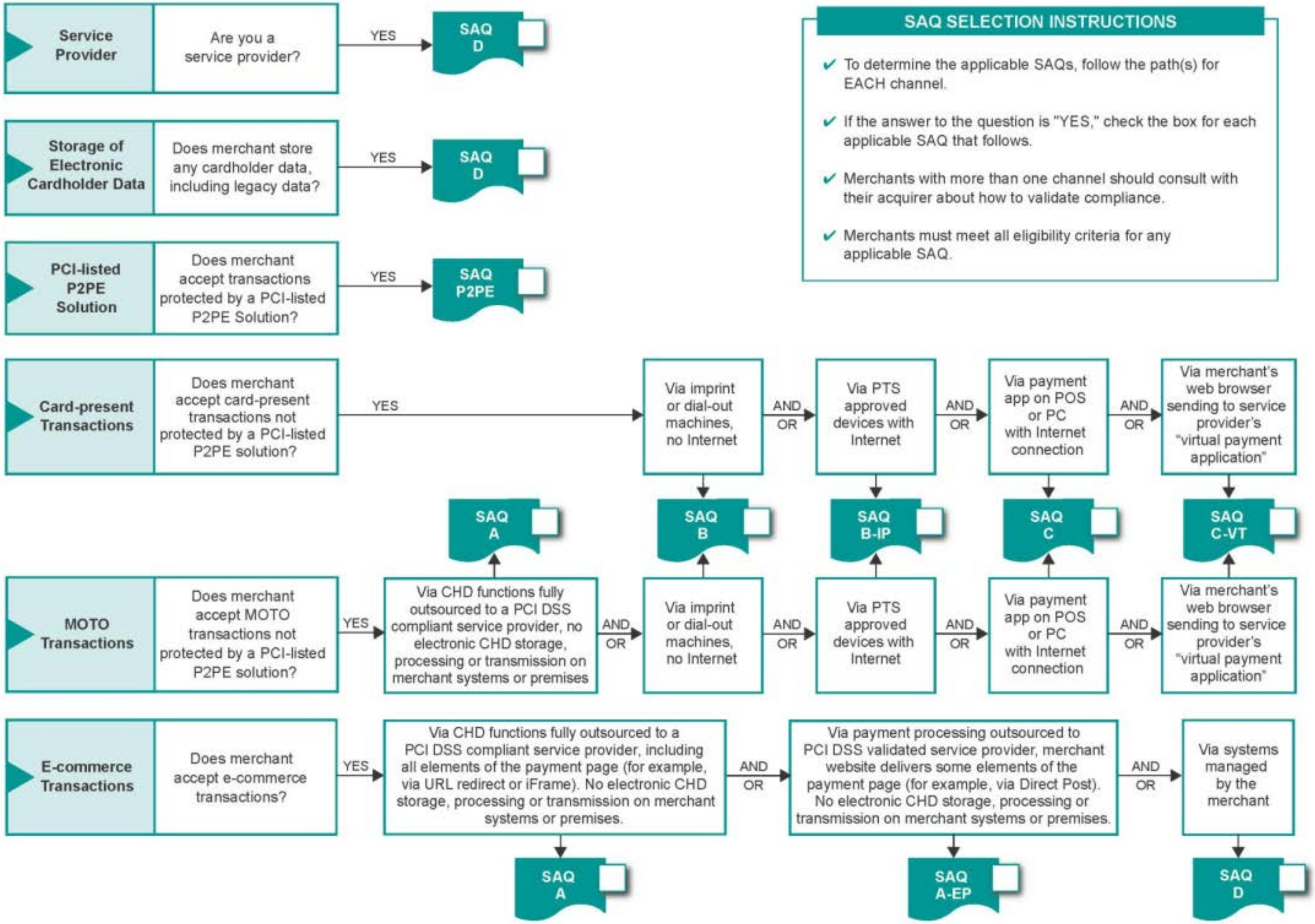
Why Is Compliance Important? - Breaches

- The consequences of a breach impacting CHD may range from $5,000 to $500,000
- A security breach and subsequent compromise of payment card data has far-reaching consequences for affected organizations, including:
  - Regulatory notification requirements,
  - Loss of reputation,
  - Loss of customers,
  - Potential financial liabilities, and
  - Litigation.

Self-Assessment

SAQ	Description
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. Stand-alone dial-up terminal merchants, no electronic cardholder data storage.
B-IP	Stand-alone network connected (non-dial-up) terminals
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage.
C-VT	Merchants using Virtual Terminals connected to the Internet, no electronic cardholder data storage.
P2PE	Merchants using a listed validated P2PE solutions
D	All other merchants (not included in descriptions for SAQs A-C above) and **all** service providers defined by a payment brand as eligible to complete an SAQ.

Which SAQ?



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 □

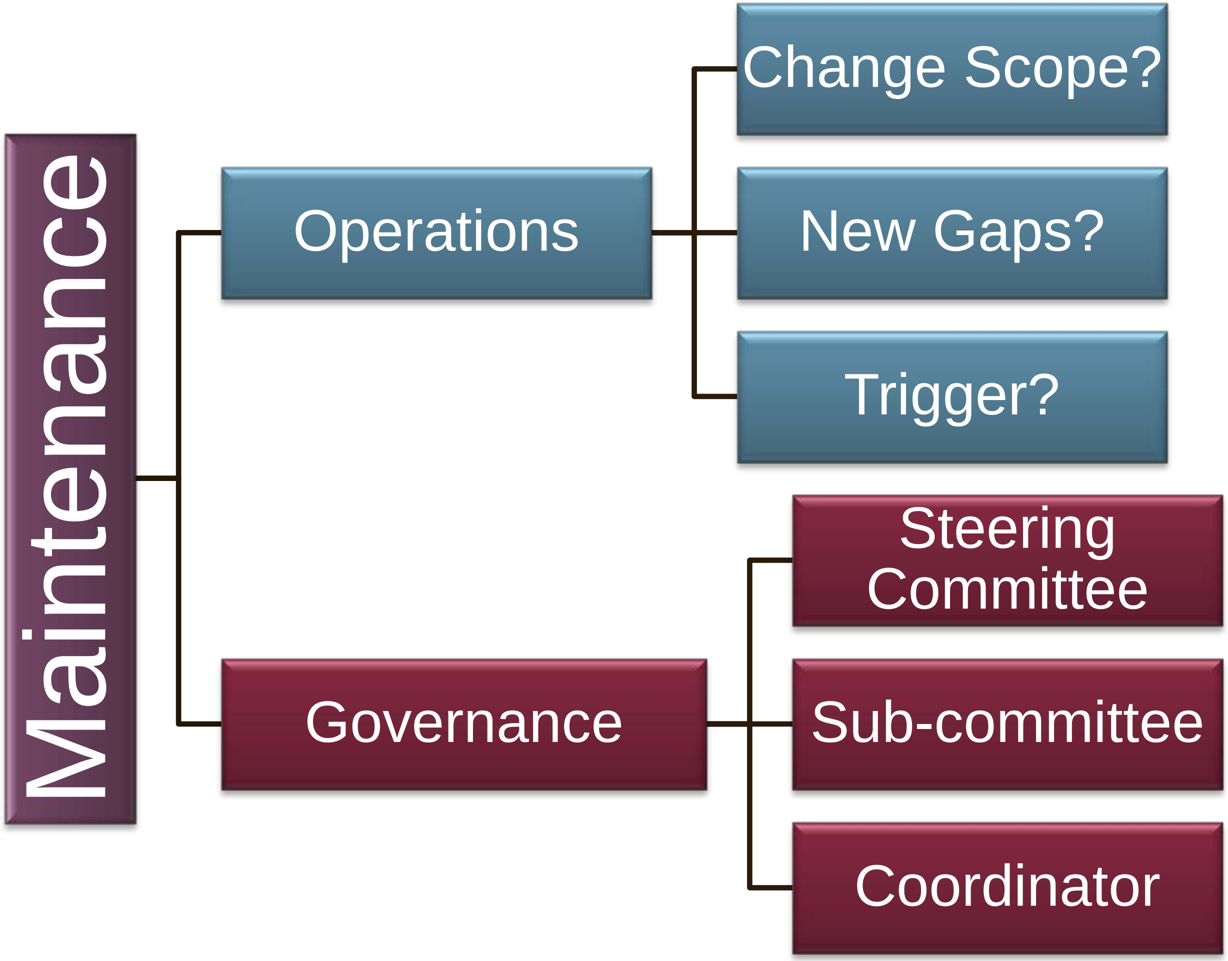
Card-present Transactions – Does merchant accept card-present transactions not protected by a PCI-listed P2PE solution? – YES →
- Via imprint or dial-out machines, no Internet → SAQ B □
- AND OR → Via PTS approved devices with Internet → SAQ B-IP □
- AND OR → Via payment app on POS or PC with Internet 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 □

Key Challenges

- Involvement and understanding extends beyond IT staff/team. Contractual obligation is usually responsibility of CFO.
- Need participation and closure with several groups within the organization: legal, finance, HR, IT.
- Internal threats greater than external threats.
- Wireless network and mobile devices (rogue APs, how to prove there is no wireless, etc.)
- Proof of compliance including logging, monitoring, testing, patching, etc.
- Managing and maintaining PCI compliance: Policies, Procedures, Information Security Awareness, etc.


Maintenance
Operations
Change Scope?
New Gaps?
Trigger?
Governance
Steering Committee
Sub-committee
Coordinator

Anatomy of a Breach

Why are we doing this?

The Ne

TJX

- BJ's Wholesale Club, DSW, Office Max, Boston Market, Barnes & Noble, Sports Authority, T.J. Maxx, Winners, and HomeSense.
- Ending in 2007, 45.6 million credit and debit card numbers were stolen over an 18 month period.
- Immediate financial loss to TJX estimated at $500,000,000.
- Reputational loss estimated at $1 Billion +
- Still remembered 5 years later.

Cause

- Gonzalez and 10 associates found WEP encrypted wireless networks while driving along U.S. Route 1 in Miami.
- WEP encryption had been known to be flawed since 2001.
- Cracking the WEP key probably took under 30 minutes.

The Walmart Breach

- Case Study: The Walmart Breach

  http://www.wired.com/threatlevel/2009/10/walmart-hack/

- Background:
- Occurred sometime between 2005 and 2006
- Discovered by accident by Walmart
- No CHD released that they were aware of

The Walmart Breach

- Discovered by accident when a server crashed.
- Investigation showed the l0phtcrack was installed on the server.
- Root Cause Analysis showed l0phtcrack was the cause of the crash.
- L0phtcrack is not an approved application.
- 2.2: Server configuration standards
- 11.5: File integrity monitoring
- 12.3.7: List of company approved products

The Walmart Breach

- Upon further investigation found 800 systems compromised
- Tracked to a remote VPN account of a former employee
- Locked that account, intruder moved to another old account
- 8.1.3 disable accounts immediately on termination
- 8.1.4 remove inactive accounts after 90 days

The Walmart Breach

- Intruder was interested in POS systems.
- Compromise went at least back to June 2005.
- This was gleaned from audit logs.
- Walmart has a large retention of log files.
- But log information was not complete.
- The compromise could not be fully reconstructed.
- 10.2.5 logging all (success, failure) use of auth mechanisms
- 10.4 time synchronization
- 10.5 secure audit logs so they won’t be altered

The Walmart Breach

Lessons

- Should not have been a surprise
- QSA highlighted these deficiencies 6 months prior
- Do your logging, keep the logs, and look at them
- When people leave remove their access
- Security is not perfect – intent is to limit damage
- Security requires diligence

PCI DSS Requirements

Requirement 0 - Scope

- Cardholder Data Environment (CDE)
- Connected-to Systems
- Must be validated each year
  - In effect you have to convince the QSA it’s accurate

Requirement 3 – Protect stored CHD

- Electronic or paper storage is in scope, but this is primarily about electronic storage
- Have a data classification and handling policy and procedure that explicitly addresses CHD and SAD.
- Don’t store SAD: CVC, Track data, PIN block
- Mask PAN when displayed
- Render PAN unreadable
- If using disk based encryption access must be managed independent from underlying OS
- Key Management

Requirement 4 – Encrypt CHD in transit

- Strong encryption when transmitting over open, public networks
- SSL, early TLS
  - Not allowed as of July 1, 2018
  - Migration plan
  - Risk mitigation plan

Requirement 4 – Encrypt CHD in transit

- No CHD over unprotected end user messaging
  - Email
  - But also SMS, IM, iMessage, tweets, FB, etc.
  - Unless you can guarantee authentication and encryption

Requirement 7 – Need to Know

- Restrict access based on need to know
- Have job roles
- Define access for those roles
- Least privilege to get their job done
- Documented approvals
- Automated system for enforcement

Requirement 8 - ID and Authentication

- Unique ID’s per person
  - This also means system, application, DB accounts
- Control addition, deletion, modification
- Revoke access immediately
- Review every 90 days
- 3rd parties: only enabled when needed, monitored when in use
- Lockout for 30 minutes after invalid attempts
- Disconnect session after 15 minutes

Requirement 8 – ID and Authentication

- Passwords, devices, biometrics
- Protect auth creds with strong crypto
- Verify users before password resets
- Change passwords every 90 days
- Minimize historical password reuse
- Change password on first use
- Authentication mechanism is unique per person – no sharing tokens

Requirement 8 – Multi-factor Authentication

- Much change here recently.
- Remote access
- Admin access to CDE remote or not
- Multi-factor NOT multi-stage
- Factors must be independent
  - Logging in with the device that also receives the onetime token is NOT independent

Requirement 9 – Physical Access

- Facility entry controls
  - Video cameras, door badge access
- Publicly accessible network jacks – No, No
- Physical access to networking equipment
- Access must be authorized (just like req 7)
- Identify and authorize visitors

Requirement 9 – Securing Media

- Physically secure all media
- Maintain strict control over storage of media
  - Inventory logs
- Maintain strict control over movement of media
  - Whether internal or externally
- Destroy when no longer needed

Requirement 9 – PINPAD Security

- Protect devices that capture payment data
- Up to date inventory
  - Make, model, location, serial number or asset ID
- Period inspections for tampering and substitution
- Train personnel on how to detect this

Requirement 12 – Education

- On hire and at least annually
- Should include periodic refreshers
- Personnel must acknowledge they have read an understood the policies that apply to them

Requirement 12 – Background Checks

- Screen personnel prior to hire
- How? Depends on your needs and their level of access
  - – Prior Job references - YES
  - – Criminal – USUALLY
  - – Credit - SOMETIMES

Requirement 12 – Incident Response

- Be prepared to respond immediately to a breach (if you notice it that is see req 10)
- The plan should be tested at least annually,
- Specific personnel should be designated to be available on a 24/7 basis,
- Staff with breach response responsibilities should be provided appropriate training.

Questions?

There are no stupid ones.