Understanding Payment Card Industry (PCI) Data Security

Office of the State Controller

November 2010

State of North Carolina

The Enemy

Major Security Breaches

- **TJ-Max**
- **Heartland**
- **Hannaford Foods**
- **BJ's Wholesale**
- **Office Max**
- **Boston Market**
- **Barnes & Noble**

Hacker

11 TJ-Max Hackers caught

- **US**
- **Ukraine**
- **China**
- **Estonia**
- **Belarus**

Fines & Lawsuits

TJ-Max - $60 Million

Major PR impact

In-house staff

70 % of all database breaches are internal

Fiscal Staff Response After a Security Breach

- I thought my IT Department was taking care of that
- I thought we had a secure website with a firewall
- I didn’t know my filing cabinets had to be secured
- I didn’t know 70% of all database breaches are internal
- I thought outsourcing to a vendor relieved me of the responsibility
- The merchant agreement with the bank didn’t specifically indicate we would be responsible for fines

Data Security Policies

- Participants in OSC's Master Services Agreement with SunTrust Merchant Services (STMS) are subject to certain policies regarding data security

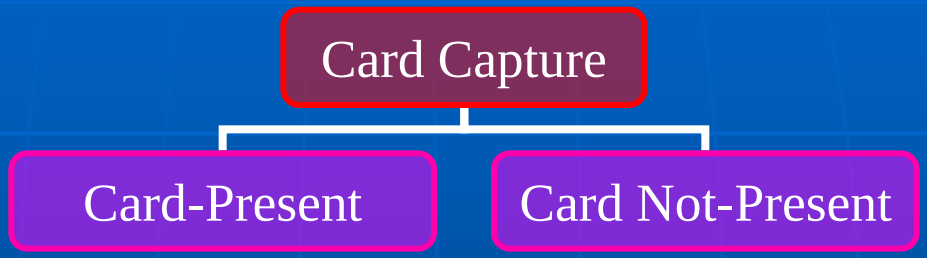
- Two specific OSC E-Commerce policies:
  - Security and Privacy of Data
  - Compliance with PCI Data Security Standards

  http://www.osc.nc.gov/SECP/SECP_Policies.html

- Policies require agencies to:
  - Adhere to Card Association Rules and standards of the PCI Data Security Council
  - Enroll in Validation Service provided by Trustwave to attest validation of compliance

Types of Card Capture

Requirements to be followed are determined primarily by the card capture channel (card capture method) being utilized, and whether a third-party service provider is used or not



Card can be swiped

- Credit Cards (with logo)
- Signature Debit Card (logo)
- PIN Debit Card (May or may not have a logo)

Card cannot be swiped

- Credit Cards (with logo)
- Signature Debit Card (logo)
- PIN-less Debit (Requires special enrollment)

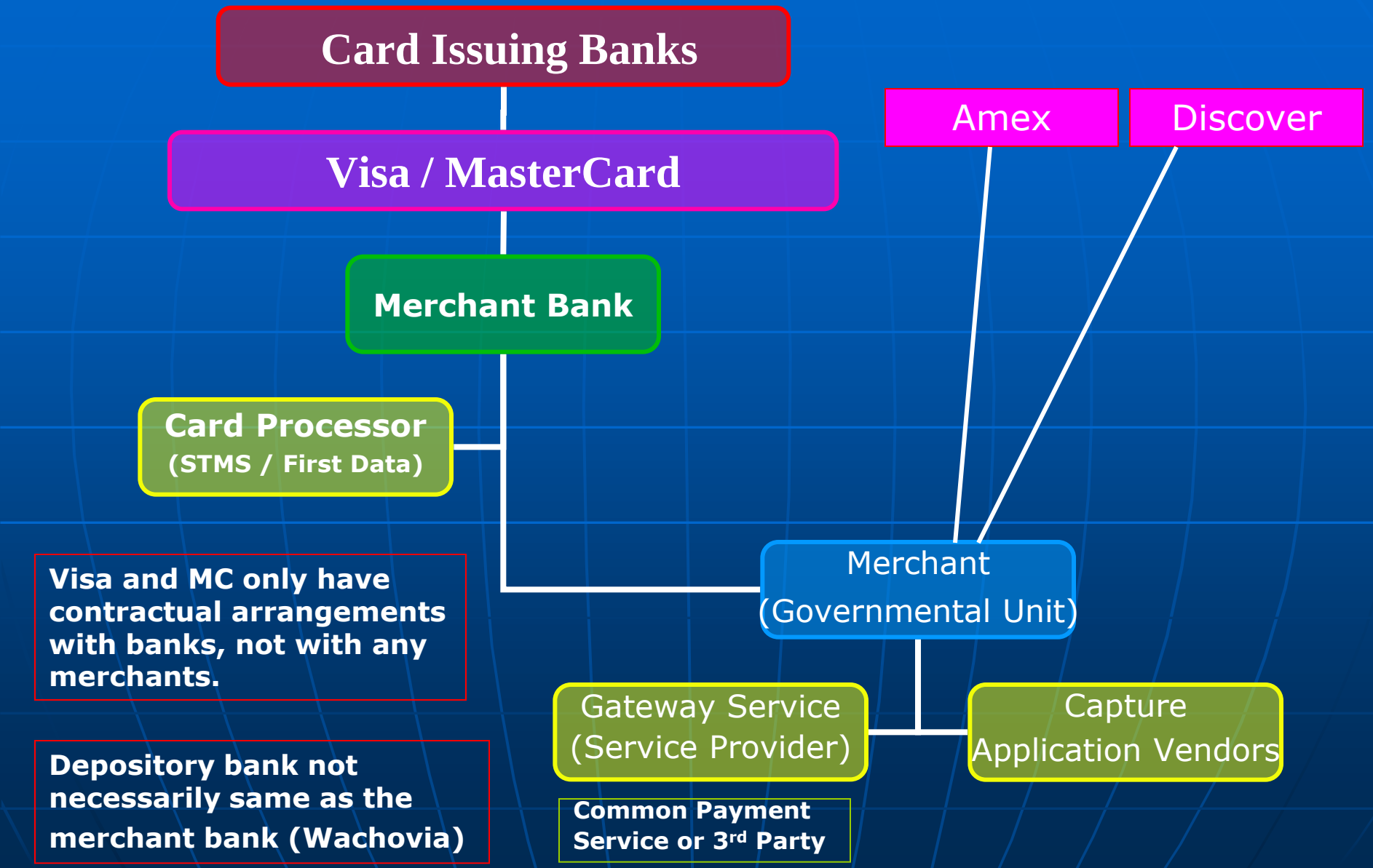
- Face-to-Face

- Through Web
- Mail Order / Telephone Order (MOTO)
- Interactive Voice Response

Capture Methods

- POS Terminal
  - Analog telephone line or via Internet connection
  - Card data swiped or keyed
  - PTS (PIN Transaction Security) applies if debit cards accepted – Triple DES Encryption
- POS Software
  - Utilizes external-facing IP Addresses (Network)
  - Card data swiped or keyed
  - PA-DSS (Payment Application Data Security Standard) applies to software purchased from vendors
- Virtual Terminal
  - Web-based POS terminal instead of POS terminal
  - Good for MOTO (Mail Order / Telephone Order)
  - Available from third-party service provider (PayPoint) or from CPS
  - Self Assessment Questionnaire C or D required
- Internet and IVR
  - In-house hosted capture application (generally an API)
  - Third-party hosted capture application (service provider) – Use of a service provider requires written agreement (Req. 12.8)

Parties to Card Transactions



Data Security Puzzle

Hacker

ASV

QSA

PA-DSS

CISP

SDP

PTS

Merchant

SAQ

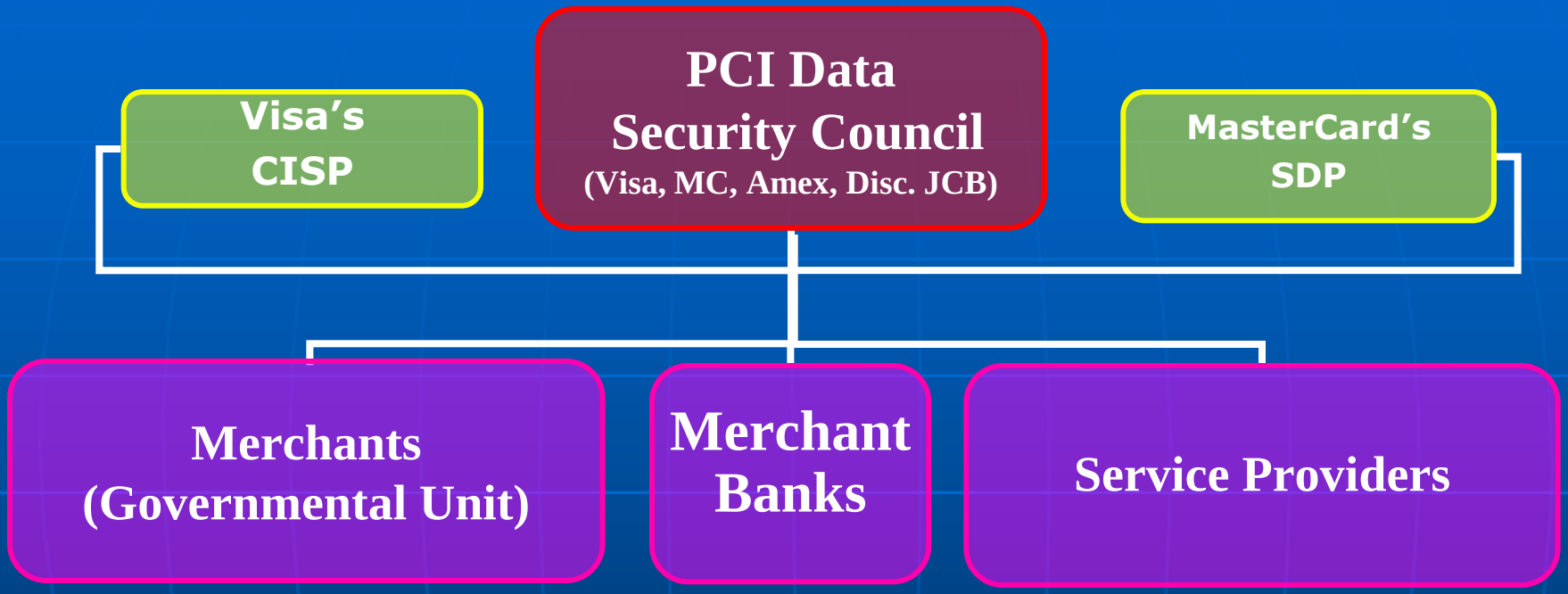
PCI DSS

NC ITPA

Data Security Terms

- CISP – Visa's Cardholder Information Security Program
- SDP – MasterCard's Site Data Protection Program
- PCI SSC – Payment Card Security Standards Council
- PCI DSS – Payment Card Industry Data Security Standard
- PCI PA-DSS – PCI Payment Application Data Security Standard
- PTS – PIN Transaction Security Standard
- NC ITPA – NC Identity Theft Protection Act (SB 1048 / 2005)
- QSA – Qualified Security Assessor (e.g., Trustwave)
- ASV – Approved Scanning Vendor (e.g., Trustwave)
- SAQ – Self Assessment Questionnaire (A, B, C, or D)
- ROC – Report on Compliance
- ISA – Internal Security Assessor

Payment Card Industry Data Security Compliance



Governmental Units (As Merchants) and their vendors are subject to:

- **Standards of the PCI Security Standards Council**
  - **PCI DSS (Payment Card Industry Data Security Standard)**
  - **PCI PA-DSS (PCI Payment Application Data Security Standard)**
  - **PTS (PIN Transaction Security Standard)**
- **Rules of the Card Associations**
  - **Visa's CISP and MasterCard's SDP – Based on Levels**
  - ***Proprietary Card Companies security policies (Amex; Discover)***

PCI DSS

Payment Card Industry Data Security Standard

- Standard that is applied to:
  - Merchants (Government Units)
  - Service Providers (Third-party vendor, gateways)
  - System (Hardware, software)
- For applications or processes that does any one of these three things:
  - Stores cardholder data
  - Transmits cardholder data
  - Processes cardholder data
- Applies to:
  - Electronic Transactions
  - Paper Transactions

What Makes Govt. Subject to PCI DSS ?

PCI Data Security Standard

Card Association Rules

Merchant Bank

Merchant Bank's Operating Guide

Merchant Agreement

Agency Participation Agreement

Governmental Unit

- **Agency Participation Agreement requires adherence to Merchant Agreement with STMS**
- **Merchant Agreement requires adherence to Operating Guide**
- **Operating Guide requires adherence to Card Association Rules**
- **Card Association Rules require adherence to PCI DSS**

Toe bone connected to the foot bone….etc.

PCI DSS Exempt Myth

- All merchants, including governmental units are subject to the standard and to card association rules
  - No exemption provided to anyone
- Sovereign immunity does not apply
  - Requirement not regulatory or statutory, but contractual
  - Card associations can be selective who they provide services to
  - Governments accept services on a voluntary basis
  - Governments agree to abide by association rules when they execute 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 (governmental unit)

Levels of Merchants

(Applies to Validation and Attestation - Not to Compliance)

	Quarterly Vulnerability Scan	Annual Self-Assessment Questionnaire or ROC
Level 1 > 6 million transactions or Suffered a hack	Scan Required for External facing IP's	Required Report On Compliance (ROC) by a Qualified Security Assessor (QSA) (On-site Audit)
Level 2 > 1 million Visa or MC transactions	Scan Required for External facing IP's	SAQ completed by internal audit staff trained via PCI SSC Internal Security Assessor (ISA) Program; or an onsite security assessment by a QSA
Level 3 > 20K e-commerce txs	Scan Required for External facing IP's	Required online SAQ A, B, C, or D
Level 4 < 20K e-commerce txs < 1 million total txs	Scan Required for External facing IP's	Required online SAQ A, B, C, or D

For participants in State's Master Services Agreement with STMS, remote validation services are provided through TrustKeeper Portal (SAQs and Vulnerability Scans)

The following services are available per Trustwave contract pricing on an optional basis:

1) Onsite security assessment by a QSA (Levels 1 & 2); or 2) Other "as needed" compliance validation services (Services require a Statement of Work)

Security Breach Fines

- Not levied by PCI Security Council
  - Fines levied by Card Associations (i.e., Visa, MasterCard)
  - Against merchant bank, which passes fines on to merchant
- Fines for security breach
  - Visa - Up to $500,000 per occurrence
  - MasterCard – Up to $500,000 per occurrence
- Amount of fines dependent upon
  - Number of card numbers stolen
  - Circumstances surrounding incident
  - Whether track data was stored or not
  - Timeliness of reporting incident
- Safe Harbor
  - Could limit amount of fine if had been validated as compliant by a QSA
  - But validation is one point in time – Don't count on

Other Security Breach Costs

- Fines levied by card associations to make notifications to all card holders and replace cards
- Costs of notifying taxpayers of incident, pursuant to the NC Identity Theft Protection Act (Chapter 75 – Article 2A)
- Forensic Investigation Costs
  - Required by card associations
  - Must used approved firm (QSA)
  - Cost approximately $10,000
- Cost associated with discontinuing accepting cards
- Cost of an annual on-site security audit
  - Once a breach has occurred, merchant is elevated to a Level 1 merchant
  - Cost approximately $15,000 - $20,000 annually

Visa's Non-Compliance Fines

Non-Compliance with PCI DSS

Merchant Level	Effective Date	Monthly Fine
1	09-30-07	$25,000
2	12-31-07	$ 5,000
3 & 4	Not yet announced	?

Non-Compliance with PCI DSS – Prohibited Data Storage (i.e., Track Data)

Effective	Level 1 Monthly Fine	Level 2 Monthly Fine	Levels 3&4 Monthly Fine
April –June 2007	$10,000	$5,000	?
July – Sept 2007	$50,000	$25,000	?
Oct '07 >	$100,000	$50,000	?

Digital Dozen

Build and Maintain a Secure Network	1) Install and maintain a firewall configuration to protect 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 and sensitive information across 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 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

Compliance-Validation-Attestation

- Compliance – Adherence to the standard
  - Applies to every merchant regardless of volume
  - Applies to both technical and business practices
- Validation – Verification that merchant is compliant with the standard
  - Depends upon type of card capture method(s) utilized
  - Two types of Validation
    - Self-Assessment Questionnaire (SAQ) Annually – Applies to every merchant
    - External Vulnerability Scanning Quarterly – Applies if external-facing IP addresses are involved (Web and POS Software) – Must be performed by a Qualified Scanning Vendor (QSV)
- Attestation – Providing proof of validation to card processor
  - Card processor reports to Visa and MasterCard
  - Attest whenever requested by the card processor

Two Components to Validation

- Annual Self Assessment Questionnaire (SAQ)
  - Four different SAQs = A, B, C, or D
  - SAQ depends upon the capture method being utilized
  - OSC provides a chart to help determine which SAQ to complete
    - http://www.osc.nc.gov/programs/pci/PCI_Applicability_to_Capture_Methods.pdf
  - Performed online via Trustwave's TrustKeeper portal (Levels 3 & 4)
  - SAQs for Level 1 and 2 merchants must be completed by PCI certified internal audit staff (See Council's site regarding "Internal Security Assessor Program"); Unless onsite assessment by a QSA
  - Community Colleges not on OSC's contract with STMS should enroll with Trustwave through NC Community College System
- External Vulnerability Scan - Quarterly
  - Required for eternal-facing IP addresses
    - Web applications
    - POS Software and POS terminals on networks (Not POS analog lines)
    - Gateways used as a "virtual terminal" (e.g., PayPoint, CPS)
  - Enroll in TrustKeeper and complete the Network Questionnaire
    - Identify IP addresses to be scanned
    - Schedule routine scans (monthly vs. quarterly)
    - "Directed Scan" can be performed after fixing a detected problem

Scans Vs. Penetration Test

There is a difference

External Vulnerability Scan

- Requirement 11.2
- Capture solutions involving external-facing IP addresses that process, transmit, or store cardholder data
- SAQ C or D applies
- Performed quarterly
- Performed by a Qualified Scanning Vendor (QSV), e.g., Trustwave

Penetration Test

- Requirement 11.3
- Capture solutions involving external-facing IP addresses, but only those that store cardholder data electronically
- SAQ D applies
- Performed annually
- Can be performed by internal, but separate organizational staff
- Refer to Council's Supplement for Requirement 11.3

Elements of Cardholder Data

Cardholder Data

- Four Elements
  - PAN
  - Cardholder Name
  - Service Code
  - Expiration Date
- Some PCI requirements only apply to PAN only, and not to all Cardholder Data

Primary Account Number

- PAN
- Full PAN can be stored, but must be protected per Requirement 3.4
- Masked-truncated PAN is out-of-scope

Sensitive Authentication Data

- Referred to as Track Data
- Three elements
  - Full Magnetic Strips
  - CVC2/CVV@/CID (Security Code)
  - PIN / PIN Block
- Can never be stored after authorization

Online Validation of Compliance

- Attestation of validation of compliance is the responsibility of the Agency's Chief Fiscal Officer (CFO)
- Each CFO may appoint a primary PCI contact to perform this function on behalf of the agency
- OSC is not responsible for attestation on behalf of any agency
- OSC contracts with Trustwave to provide PCI Validation Services to the various participants in the State's MSA
- Validation service facilitated through online TrustKeeper portal
- Each participant is required to enroll in TrustKeeper at the "chain" level, not the "outlet" level
- Two options upon enrollment – for Remote Validation Services:
  - Self-Assessment Questionnaire Only
  - Self-Assessment Questionnaire and Vulnerability Scanning
- Reports of validation results are available to:
  - STMS (Card Processor)
  - The appropriate central oversight agency (i.e., ITS, UNC-GA, NCCCS)
- Any non-compliance issues that the reports may indicate will be addressed with the participant by STMS
- The consequences of non-compliance could include:
  - Fines by Visa and/or MasterCard
  - Suspension or termination of services from STMS

Service Providers

- Responsibility of the merchant to utilize compliant service providers
  - If service provider not compliant, then merchant is not compliant
  - Any fines for breaches accessed to merchant not to the service provider
- Examples of Service Providers
  - Gateway Service Provider (e.g., PayPoint, PayPal, Yahoo, TouchNet, etc.)
  - Web Hosting Service Provider
  - Backup Storage Service Provider
- PCI Requirement 12.8 applies, requiring merchant to "manage" the service provider:
  - Maintaining a "written agreement" specifying the service provider's responsibility for compliance
  - Performing due diligence to ensure PCI compliance prior to engagement
  - Monitoring the service provider's compliance status
- Monitoring the Service Provider
  - Some vendor are registered as compliant by Visa or MC, but not all
  - Merchant should obtain "evidence" of compliance from vendor (e.g., Report on Compliance – ROC)
  - Sample addendum for Requirement 12.8 available on OSC's website
  - Merchant cannot answer SAQ truthfully if requirements not met

PCI PA-DSS
Payment Application Data Security Standard

- Separate standard than the PCI Data Security Standard
- Formerly known as Payment Application Best Practice (PABP)
- Applies to vendors' application software (e.g., point of sale software) that are licensed and sold to merchants
- Does not apply to customized applications developed for a single merchant
- List of approved applications is available on both Visa's and PCI Council's websites
- Applications not certified by July 1, 2010 subject to being terminated
- There are more breaches of software applications than web applications

PTS
PIN Transaction Security Standard

- Separate standard than the PCI Data Security Standard
- Formerly known as PCI PED
- Applies to POS Terminals that processes PIN-based debit cards
- Requires Triple DES Encryption
- POS terminals not compliant by July 1, 2010 must be replaced
- Two different lists of compliant POS Terminals
  - PCI PEDs – on PCI Council's Website
  - Pre-PCI PED – on Visa's Website
- Pre-PCI PED terminals not replaced by December 2014 subject to fines by Visa

Security Incident Plan

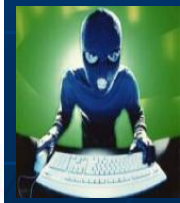
- Requirements of:
  - OSC's policy- "Merchant Cards Security Incident Plan"
  - Card Association Rules
  - Requirement number 12 of the PCI DSS

- Basic points
  - Must have a formal plan
  - Applies to both technology and paper breaches
  - OSC must be notified in all cases - immediately
  - If participant is subject to ITS oversight, ITS policy applies
  - OSC coordinates reporting to card associations through STMS
  - Card associations take into consideration timeliness of reporting when determining fines for breach

What Could Be Done Better?

- Store Less Data
  - Don't store cardholder data unless a compelling business reason to do so
  - Determine where credit card data exists in your organization, what it is used for, and whether it is needed there
  - Eliminate "shadow databases" (Excel worksheets, etc)
  - View online reports, don't download them (downloading = storing)
  - Ensure your POS systems don't store magnetic stripe data by default
  - Retaining of CVV2 data and PIN subsequent to authorization is "No-No"
  - Ensure written agreement in place when utilizing service providers (R.12.8)
- Better Access Controls
  - Limit cardholder data only to employees with "need to know"
  - Segment databases – thereby limiting scope of PCI
  - Implement requirements specified in the Standard, as identified in the annual Self Assessment Questionnaire (SAQ)
- Establish Policies and Procedures
  - Provide annual employee awareness and training
  - Develop an Incident Reporting Plan
- Establish Internal Committee
  - Made up of both IT staff and business staff

Barn Door



Resources

PCI Security Council Web Site
https://www.pcisecuritystandards.org/

Visa's CISP Web Site
http://usa.visa.com/merchants/risk_management/cisp.html

MasterCard SDP Web Site
http://www.mastercard.com/us/sdp/index.html

State Controller's Web Site
http://www.osc.nc.gov/programs/risk_mitigation_pci.html

UNC School of Government - Center for Public Technology
Shannon Tufts - tufts@sog.unc.edu (Local Units of Govt)

David C. Reavis
Director of E-Commerce Initiatives
NC Office of the State Controller
(919) 871-6483
david.reavis@osc.nc.gov

Support Services Center
(919) 707-0795