Monday, October 20
2:30 pm-4:00 pm

207 Payment Card Industry Requirements- How to Protect Your Credit Card Data

David M. Goldwin
Vice President and Divisional Counsel
TSYS Acquiring Solutions LLC

Julie Krueger
Vice President and PCI Security Standards Council Representative
JCB International Credit Card Company (Americas)

Petra Vorwig
Attorney
Steptoe & Johnson LLP

Faculty Biographies

David Goldwin

David Goldwin is vice president and divisional counsel at TSYS Acquiring Solutions, LLC, a credit card transaction processor headquartered in Tempe, AZ. At TSYS, Mr. Goldwin oversees all legal activity, including preparing and executing contracts, managing the company's intellectual property, assisting in statutory and card brand compliance efforts, and managing all litigation.

Prior to joining TSYS, Mr. Goldwin worked in legal and project management for numerous companies within the merchant acquiring industry, including Harbridge Merchant Services, Card Establishment Services, and First Data. Mr. Goldwin also served as the general counsel for a healthcare information services company, MedE America, overseeing an initial public offering and subsequent acquisition by WebM.D.

Mr. Goldwin currently serves on the Electronic Transaction Association's government relations committee.

Julie Krueger

Julie Krueger is the vice president of JCB Credit Card Company on the payment card industry (PCI) security standards council in Los Angeles. Her department encompasses the PCI data security standard, the payment application data security standard, and pin entry device security requirements. Ms. Krueger also represents JCB in several EMVCo LLC global smart card initiatives. Within the US market, Ms. Krueger is responsible for ensuring successful implementations of new JCB products and technologies, including contactless and EMV smart cards as well as e-commerce authentication solutions.

Prior to joining JCB, Ms. Krueger worked for a PKI (Public Key Infrastructure) security company as well as for several semiconductor companies, including Intel Corporation. Ms. Krueger has also served as the executive director of the Smart Card Forum, and she has been involved with financial payment security and smart cards for over 20 years.

Petra Vorwig

Petra A. Vorwig is an attorney in the Washington, DC office of Steptoe & Johnson LLP, where she is a member of the international and technology departments.

As a member of Steptoe's international department, Ms. Vorwig advises clients on export control and economic sanctions laws and regulations. Her export/sanctions practice covers operational and transactional counseling, licensing and advisory opinions, internal investigations, enforcement matters, and regulatory policy. Ms. Vorwig has experience dealing with the principal US agencies administering these regulatory programs, including the Departments of Commerce, State, and Treasury. Ms. Vorwig also advises companies on encryption import, export, and use laws and regulations under US rules. Her experience in the encryption area includes encryption licensing and product classifications.

As a member of the technology department, Ms. Vorwig provides legal advice on matters involving privacy and data security. She has experience counseling clients on their responsibilities to protect personal information maintained on electronic networks and potential liability in the event those networks are breached.

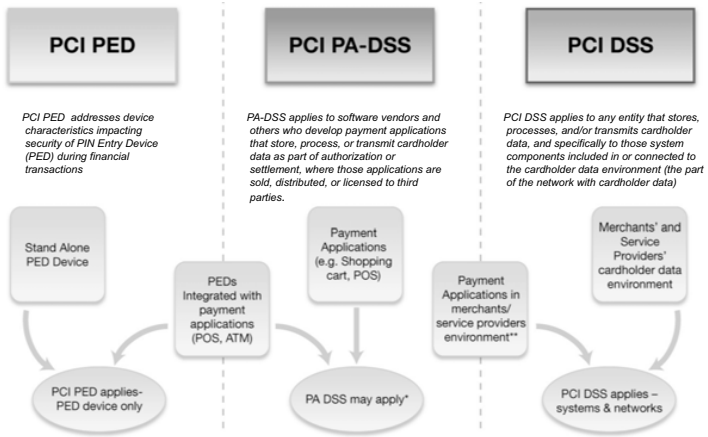
Ms. Vorwig also represents domestic and foreign telecommunications clients, who provide international and domestic telephone, wireless, and satellite telecommunications services, before the FCC and other federal government agencies. She has advised clients on a variety of issues relating to mergers and acquisitions, and has prepared comments in numerous FCC rulemaking proceedings on a wide variety of issues affecting the telecommunications industry, including spectrum allocation and service rules. Ms. Vorwig also has extensive experience in licensing proceedings for satellite systems, earth stations, terrestrial wireless carriers, international common carriers, and submarine cable operators.

Payment Card Industry (PCI) Security Standards

Payment Card Industry Security Standards

Julie Krueger

PCI SSC - The Standards



The PCI Security Standards Council

- An open global forum, launched in 2006, responsible for the development, management, education, and awareness of the PCI Security Standards, including:
  - Data Security Standard (DSS)
  - Payment Application Data Security Standard (PA-DSS)
  - Pin-Entry Device (PED)

The PCI Security Standards Council Founders

AMERICAN EXPRESS

VISA

PCI Security Standards Council

DISCOVER NETWORK

MasterCard Worldwide

JCB JCB CARDS

PCI Security Standard Council (SSC)

- Over 500 Participating Organizations (POs) worldwide
- 1,500 QSA Assessors trained and certified
- New PED, PA-DSS and DSS V1.2 Standards announced
- Started Special Interest Group Program
- Influential Outreach and Education Program
- Board of Advisors elected and working (i.e. Task Forces)

Participating Organizations

Categories

34% Merchant

15% Processor

8% Financial Institution

2% Multiple

41% Other

Global Participation & Representation

Over 500 organizations worldwide are involved as POs

United States	73%
Asia Pacific	2%
Canada	6%
Europe	16%
Latin America/ Caribbean	1%
Central Europe /Middle East /Africa	2%

Board of Advisors

- **Financial Institutions**
  - Bank of America
  - JP Morgan Chase and Co.
  - Citibank N.A., Global Consumer Group
  - Commonwealth Bank of Australia
  - The Royal Bank of Scotland
- **Merchants**
  - British Airways, plc
  - Exxon Mobil Corporation
  - McDonalds Corporation
  - Microsoft
  - Tesco Stores Ltd.
  - Wal-Mart Stores, Inc.
- **Processors**
  - Chase Paymentech Solutions
  - First Data Corporation
  - Interac Association
  - Moneris Solutions Corporation
  - SERVICIOS ELECTRONICOS GLOBALES S.A. DE C.V.
  - TSYS Acquiring Solutions
- **Associations & Vendors**
  - APACS
  - EPC
  - PayPal, Inc.
  - VeriFone, Inc.

Roles and Responsibilities of the Council

PCI SSC….

- Is an Independent Industry Standard
- Manages the technical and business requirements for how payment data should be stored and protected
- Maintains List of Qualified PCI Assessors
  - QSAs, ASVs

PCI SSC Does Not…

- Manage or drive Compliance
  - Each brand continues to maintain its own compliance programs
    - Identifies stakeholders that need to validate compliance
    - Definitions of Validation Levels
    - Fines and Fees

Threat Landscape

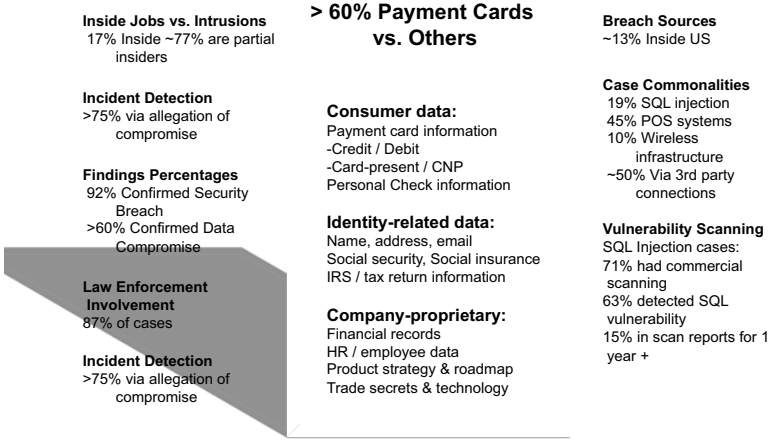
Implementing the standard is a Journey…… Not a Destination

- Threats in one month: August 2007
  - 89% of email was spam (new record)
  - Trojans made up 78% of new malware
  - 264,133 new zombies detected
  - Average of 11,906 new malicious websites found daily

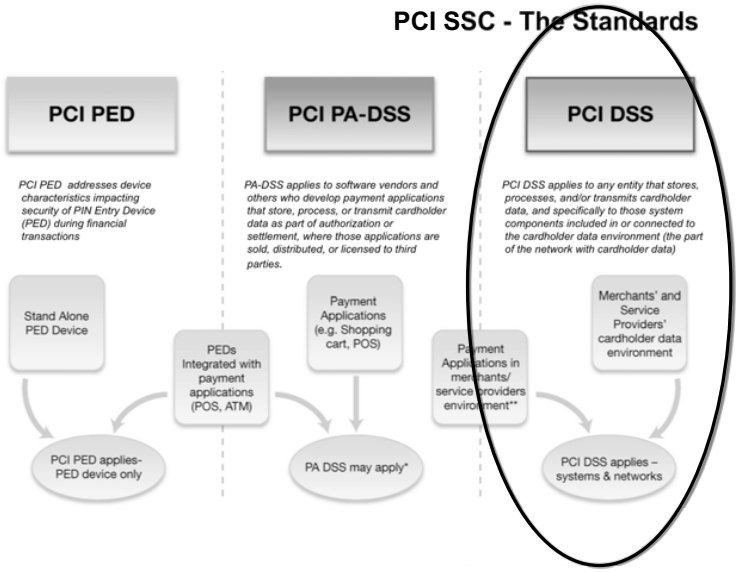
Resources Provided by Council

- Security Standards and Supporting Documents
- Frequently Asked Questions
- List of Approved QSAs, ASVs, PED Labs
- Education and Outreach Programs
- Participating Organization Membership, Community Meetings, Feedback
- One Global Voice for the Industry

Forensics Statistics



PCI SSC - The Standards



The PCI Data Security Standard

- The PCI DSS version 1.2, released in September 2008, is an updated set of comprehensive requirements for enhancing cardholder data security
- The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures
- This comprehensive standard is intended to help organizations proactively protect cardholder data

The Five Stages of Grief

•**Denial**	**It doesn't apply to me** *PCI compliance is mandatory*
•**Anger**	**It isn't fair** *PCI applies to all parties in the payment process*
•**Bargaining**	**I'll do some of it** *Compliance is "pass / fail"*
•**Depression**	**I'll never get there** *Many merchants already have*
•**Acceptance**	**It'll be OK** *PCI doesn't introduce any new, alien concepts*

The PCI Data Security Standard

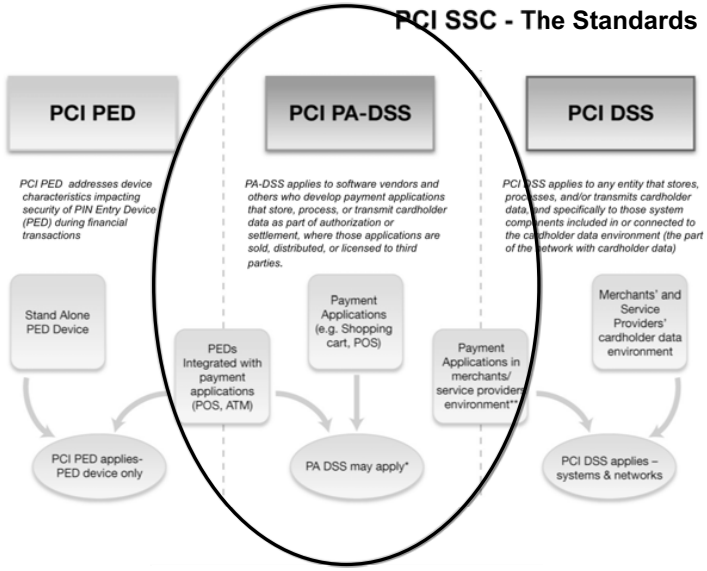
Six Goals, Twelve Requirements

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 data 4. Encrypt transmission of cardholder data across open, 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 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

Data Storage Clarification

	Component	Storage Permitted	Protection Required	Encryption Required**
Cardholder Data	PAN	YES	YES	YES
	Expiration Date*	YES	YES	NO
	Service Code*	YES	YES	NO
	Cardholder Name*	YES	YES	NO
Sensitive Authentication Data	Full Magnetic Strip	NO	N/A	N/A
	CVC2/CVV/CID	NO	N/A	N/A
	PIN	NO	N/A	N/A

PCI SSC - The Standards



Top PCI DSS Violations

Requirement 1: Install and maintain a firewall to protect cardholder data

Requirement 3: Protect stored data

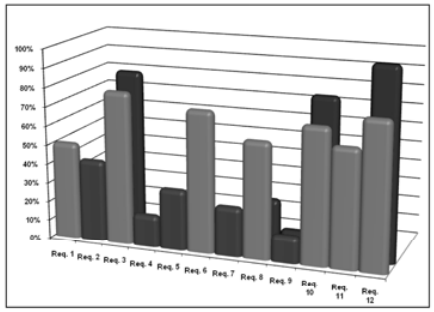
Requirement 6: Develop and maintain secure systems and applications

Requirement 8: Assign a unique ID to each person with computer access

Requirement 10: Track and monitor access to network and card data

Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security



Violations >50% Found During Forensic Investigations

Violations <50% Found During Forensic Investigations

Violations Found During Initial PCI DSS Audits

The Payment Application Data Security Standard

- Based on Visa USA's PABP, the PA -DSS is a comprehensive set of requirements designed for payment application software vendors to facilitate their customers' PCI DSS compliance
- This comprehensive standard is intended to help organizations minimize the potential for security breaches due to flawed payment applications, leading to compromise of full magnetic stripe data
- Distinct from but aligned with PCI DSS

The Payment Application Data Security Standard

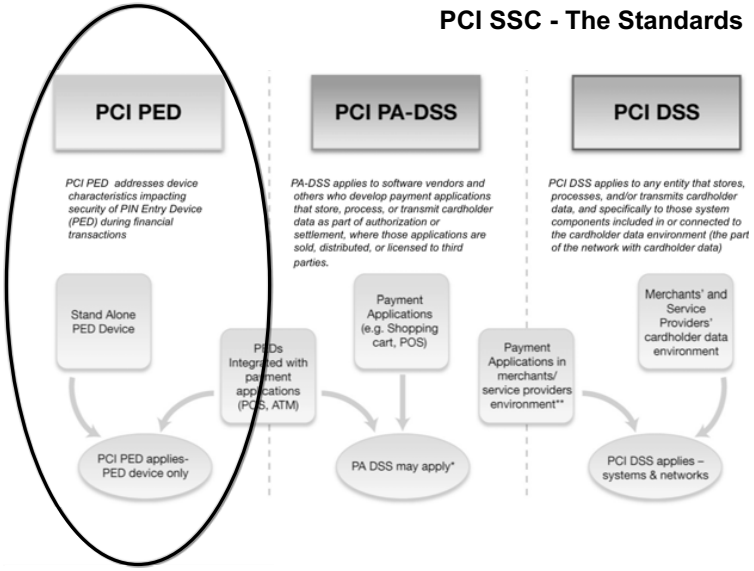
Fourteen Requirements…Protecting Payment Application Transactions

Do not retain full magnetic strip, card validation code or value (CAV2, CID, CVC2, CVV2) or PIN block data
Provide secure password features
Protect stored cardholder data
Log Application Activity
Develop Secure Applications
Protect wireless transmissions
Test Applications to address vulnerabilities
Facilitate secure network implementation
Cardholder data must never be stored on a server connected to the Internet
Facilitate secure remote software updates
Facilitate secure remote access to application
Encrypt sensitive traffic over public networks
Encrypt all non-console administrative access
Maintain instructional documentation and training programs for customers, resellers, and integrators

The PIN Entry Device Requirements

- These requirements are divided into the following categories:
- Device Characteristics:
  - Physical Security Characteristics
  - Logical Security Characteristics
- Device Management
  - Device Management During Mft.
  - Device Management Between Mft. and Initial Key Loading
  - Considers how the PED is produced, controlled, transported, stored and used throughout its life cycle. If the device is not properly managed, unauthorized modifications might be made to its physical or logical security characteristics.

PCI SSC - The Standards



PIN Entry Device Requirements

Physical Attributes

- Attributes that deter physical Attacks
  - ex penetration of device to determine key(s)
  - Planting a PIN disclosing bug within

Logical Attributes

- Logical security characteristics include functional capabilities that preclude:
  - Allowing device to output clear text PIN encryption key

The PED Security Requirements are designed to secure personal identification number (PIN)-based transactions globally and applies to devices that accept PIN entry for all PIN-based transactions

QSAs

- Organizations that validate an entity's adherence to PCI DSS requirements are known as Qualified Security Assessors (QSAs).
- Over 150 QSA companies
- To find more about the program:
  - https://www.pcisecuritystandards.org/resources/qualified_security_assessors.htm

PA-QSAs

- Organizations that validate an entity's adherence to PCI PA-DSS requirements are known as PA-QSA
- Over 20 PA-QSA companies
- To find more about the program:
  - https://www.pcisecuritystandards.org/resources/qualified_security_assessors.htm

ASVs

- Organizations that validate adherence by performing vulnerability scans of internet facing environments of merchants and service providers are known as Approved Scanning Vendors (ASVs).
- Over 130 ASVs
- https://www.pcisecuritystandards.org/resources/approved_scanning_vendors.htm

PED Vendors

- Organizations that manufacture PIN acceptance devices for use in the acceptance of PINs during a financial transaction using a payment card
- Approximately seventy vendors with over 170 approved devices
- https://www.pcisecuritystandards.org/PIN

PCI Compliance

What the Card Brands Require (and the cost of ignoring them)

David Goldwin
VP/Divisional Counsel – TSYS Acquiring Solutions, LLC

The Players

- Brands
- Banks
- Merchants
- Assessors
- Service Providers
- Legislatures?

PCI Council sets the Standards…

But the Card Brands enforce the rules

Cost Of Non Compliance

- TJX - $40.9 million to issuers for data breach, *and* TJX Acquirer Fifth Third fined an additional $880,000.
- CardSystem Solutions, Inc. – 40 million card numbers allegedly stolen. CSSI sold to Pay by Touch in 2005, now in bankruptcy (Solidus Networks). Also sued by the FTC, settled 2/23/06.

How we arrived at the Current State

Card Brands independently developed rules and enforced them.

Amex – Data Security Operating Policy (DSOP)
Discover – Discover Information Security & Compliance (DISC)
MasterCard - Site Data Protection (SDP)
Visa – Cardholder Information Security Policy (CISP)

Multiple rules could not be simultaneously enforced.

PCI – Announced September, 2006

First Order of Business: Who has to Comply by When?

Card Brands Set requirements for Merchants and Service Providers.

Different Missions for PCI and the Card Brands

- PCI – "The PCI Security Standards Council's mission is to enhance payment account data security by driving education and awareness of the PCI Security Standards. The organization was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc."
- MasterCard – "The MasterCard SDP Program is designed to encourage members, merchants, Third Party Processors (TPPs), and Data Storage Entities (DSEs) to protect against account data compromises."

American Express

DSOP Merchant Levels

Level 1 – 2.5 Million Amex transactions annually, any merchant who has had a data breach, or "other" at Amex's discretion.
Must have annual onsite security audit, and quarterly network scan.

Level 2 – 50,000 – 2.5 million Amex transactions annually.
Must have a quarterly network scan.

Level 3 – Less than 50,000 Amex transactions annually, a quarterly network scan is "strongly recommended".

Fines for Noncompliance

Non-Validation Fees – "Merchants will be assessed non-validation fees and their Card Acceptance Agreement may also be terminated if they do not fulfill these requirements or fail to provide the mandatory Validation Documentation."

Failure to timely submit Validation Documentation - $50,000.

Failure to submit Validation Documentation within 30 days following due date - $150,000.

Failure to submit Validation Documentation within 60 days following due date - $200,000, possible termination of Amex acceptance privileges.

Fines for Noncompliance

MasterCard – Fines Acquirer, not the merchant, for the merchant's noncompliance.

Level 1 Merchants - $25,000
Level 2 Merchants - $10,000
Level 3 Merchants - $5,000.
"MasterCard may assess an acquirer up to $500,000 in aggregate for any continuing violations.

Visa – Fines the member per violation in rolling 12 months.

First Violation - $50,000
Second Violation - $100,000
Third or subsequent Violations - "At the discretion of Visa U.S.A.".

Merchant Levels

Level	Definition
1	Any merchant, regardless of acceptance channel, processing over 6,000,000 transactions per year. Any merchant that the card brand, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the system.
2	Any merchant, regardless of acceptance channel, processing 1,000,000 to 6,000,000 transactions per year.
3	Any merchant processing 20,000 to 1,000,000 e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 e-commerce transactions per year, and all other merchants-regardless of acceptance channel-processing up to 1,000,000 transactions per year.

Compliance Dates for Merchants

Level 1 Merchants - 6/30/05 - Annual Onsite Review, Quarterly Scans.

Level 2 Merchants -12/31/08 - Annual Self Assessment, Quarterly Scans.

Level 3 Merchants - 6/30/05 - Annual Self Assessment, Quarterly Scans.

Level 4 Merchants – TBD – Consult Acquirer.

Assessors and Scans

Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV) – Both certified by the PCI SSC.

The QSA must demonstrate security audit expertise, work history, and industry experience.

The ASV must have experience and knowledge with information security vulnerability, assessment engagements and penetration testing, preferably related to payment systems.

Service Provider Requirements

Level 1 and Level 2 Service Providers must have an annual on site security audit by a QSA, and have quarterly network scans performed by a QSV.

Level 3 Service Providers must perform an annual self-assessment, and have quarterly network scans performed by a QSV.

Service Providers

Level 1 - All processors (member and nonmember) and all payment gateways. Payment gateways are agents or service provider that store, processes, and/or transmit cardholder data as part of a payment transaction.

Level 2 - Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 accounts/ transactions annually.

Level 3 - Any service provider that is not in Level 1 and stores, processes, or transmits fewer than 1,000,000 accounts/ transactions annually.

What do you have to do if there is a Breach?

1. Immediately contain and limit the exposure. Prevent further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information.
2. Alert all necessary parties immediately. This includes internal security resources, the acquirer, and law enforcement.
3. Provide all compromised account information to your merchant bank within 10 business days. All potentially compromised accounts must be provided and transmitted as instructed by your merchant bank.
4. Within 3 business days of the reported compromise, provide an Incident Report document to your merchant bank.

PCI – PA DSS (Payment Applications)

Applications – What Are they? Any third-party payment application utilized by a merchant or agent that is involved in the authorization or settlement of a payment card transaction.

What is Covered? Point of sale, middle-ware, shopping carts/store fronts, handheld devices, payment kiosks, ATMs.

What is not Covered? In-house use only developed applications, stand-alone POS terminals, database software, web server software.

What about standalone POS terminals? They are not covered provided;

- The terminal has no connections to any of the merchant's systems or networks
- The terminal connects to the acquirer or processor
- The terminal vendor provides secure remote access, updates, maintenance and troubleshooting
- The following are never stored post authorization: the full contents from the magnetic stripe (that is on the back of a card, in a chip, or elsewhere), CVV, CVV2, PIN or encrypted PIN block

Legislatures!?

Texas HB 3222 : BUSINESS DUTY TO PROTECT AND SAFEGUARD SENSITIVE PERSONAL INFORMATION.

Passed the Texas House in May 2007 by a vote of 139 – 0. Now sitting in committee in the Senate.

Provides: "(c) A business that, in the regular course of business and in connection with an access device, collects sensitive personal information or stores or maintains sensitive personal information in a structured database or unstructured files must comply with payment card industry data security standards."

Who Enforces this? "(e) A financial institution may bring an action against a business that is subject to a breach of system security if, at the time of the breach, the business is in violation of Subsection (c). A court may not certify an action brought under this subsection as a class action."

PCI PA DSS Timeframes

1/1/08 - Phase 1. Newly boarded merchants must not use known vulnerable payment application and Service Providers must not certify known vulnerable payment applications.

7/1/08 - Phase 2. Service Providers must certify only PA-DSS compliant payment applications to their platforms.

10/1/08 - Phase 3. Newly boarded Level 3 and 4 merchants must be PCI DSS compliant or utilize PA-DSS compliant payment applications.

10/1/09 - Phase 4. Service Providers must decertify all known vulnerable payment applications.

7/1/10 - Phase 5. Acquirers must ensure their merchants and Service Providers use PA-DSS compliant payment applications.

Texas HB 3222 (cont'd.)

How do you know if you are compliant?

"(g) A presumption that a business has complied with Subsection (c) exists if:

(1) the business contracts for or otherwise uses the services of a third party to collect, maintain, or store sensitive personal information in connection with an access device;

(2) the business requires that the third party attest to or offer proof of compliance with payment card industry data security standards; and

(3) the business contractually requires the third party's continued compliance with payment card industry data security standards."

Consider the following;

There is more than one way to comply with PCI DSS, i.e. you use compensating controls vs. encryption. Have you complied with HB 3222?

A third party used by the merchant was PCI Compliant at the time of contract, but allowed compliance to lapse. Is the merchant or the third party liable?

Most compromises involve a third party criminal act. Does the intervening criminal act insulate the merchant from liability?

You Know What PCI Is: Now What?

Steps to Implementing and Maintaining PCI Compliance

Presented By: Petra A. Vorwig

Sources of Liability

- Federal Law
  - Federal Trade Commission Act
  - Gramm-Leach-Bliley Act
  - Fair and Accurate Credit Transactions Act
- State Law
  - Financial Privacy Laws
  - Credit Card Privacy Laws
    - Minnesota mandates PCI compliance
  - Data Security Laws
  - Breach Notification Laws
  - Tort
- Contractual Obligations to Maintain PCI Compliance
  - Indemnification for penalties applied to your acquiring bank
- Restrictions Imposed by Payment Card Company

Mitigating Your Risk

- Contract with recognized PCI compliant vendors and processors
- Incorporate on-going PCI compliance into your contracts
- Include indemnification clauses for damages resulting from a breach or other non-compliant activities
  - Payment card imposed penalties passed down from your acquiring bank
  - Cost to remedy damage to card holders
  - Cost to defend consumer lawsuits
  - Cost to your business

Ensuring Internal Compliance

- Incorporate PCI compliance into your broader data security program
- Ensure every level of your business from CEO to cashier is committed to protecting consumer information
- Assign compliance responsibility to individuals at the appropriate level in every relevant business unit (e.g. IT, Legal, HR, Customer Relations)
- Enforce the message
- Enforce the program

Establishing a Compliance Program

- Spell out responsibilities for securing consumer information at each level of your business
  - IT personnel
  - Payment processors
  - Cashiers
- Identify individuals in the relevant businesses responsible for completing mandatory reports or questionnaires
- Establish schedule for quarterly scans
- Establish procedures for recognizing a breach and informing appropriate IT and Legal personnel
- Require subcontractors or other service providers to adhere to the program

Compliance Audits and Program Revisions

- Conduct regular audits of your program
  - These are additional to mandatory reporting or self-assessment questionnaires
  - Identify areas of non-compliance or potential weaknesses
- Routinely revise your program to address weaknesses or to improve overall strength and efficiency

Training

- Internal Training
  - Annual for all employees
  - More detailed training on a more frequent basis for employees involved in maintaining compliant systems
- External Training
  - Attend PCI Council training
  - Ensure new information is disseminated to the right people

What Happens If a Breach Occurs?

- Each payment card may have specific response procedures
- Conduct a thorough investigation
- Alert affected parties
  - Your internal information security personnel
  - Financial institutions
  - Payment card's fraud control group
    - Failure to alert may result in a fine
  - Local office of the Secret Service and FBI
- Monitoring may be conducted by payment card or financial institution
- Additional notifications may be required if consumer personal information is compromised