



Payment Card Industry Data Security Standards (PCI DSS): An IT Internal Audit Perspective

**ISACA Hawaii
Chapter Luncheon**

Thursday, February 12, 2009

Carey Carpenter
Senior Manager
Deloitte & Touche LLP



The Fine Print

This presentation contains general information only and Deloitte & Touche LLP is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte & Touche LLP, its affiliates and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.

Today's Discussion

- Introduction to Credit Card Payments
- PCI DSS
- Compliance Validation
- Internal Audit's Role
- Challenges and Common Compliance Issues

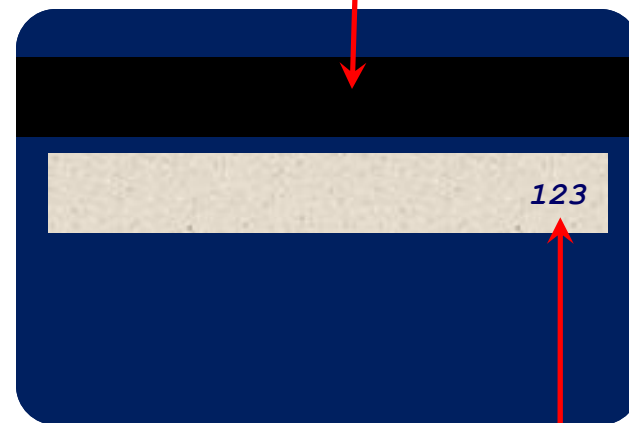
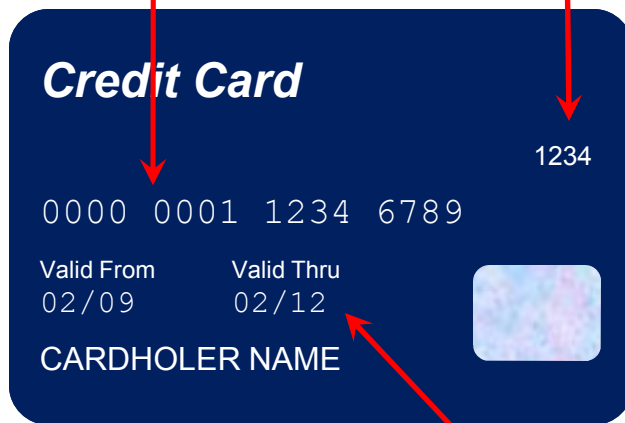
Introduction to Credit Card Payments

Credit Card

Credit Card Number
(PAN)

CID
(American Express)

Track Data (Tracks 1 & 2)
on magnetic stripe



Expiration Date

CAV2/CID/CVC2/CVV2

Introduction to Credit Card Payments

Credit Card (Cont.)

What data is stored on a credit card and why is it important?



Magnetic Stripe (i.e., “track data”)

- Contains sensitive data including cardholder name, account number, expiration date, CVV, and PIN verification value (PVV).
- Full track information cannot be stored.
- CVV and PVV values cannot be stored.
- Elements of the track that may be retained as required by business needs are: cardholder name, account number, expiration date and service code.
- If stored and compromised, the data can enable production of counterfeit cards.

Card Validation Value or Code (e.g., CVV2, CVC2, CID, CAV2)

- A 3 or 4 digit code that helps mail order/telephone order (MO/TO) and e-Commerce merchants validate that the customer has the card in their possession and that the account is legitimate.
- This information cannot be stored.
- If stored and compromised, the data can enable fraudulent online transactions.

PIN values key entered into PIN PAD devices for debit transactions also cannot be stored, even if encrypted (e.g., PIN blocks).

Introduction to Credit Card Payments

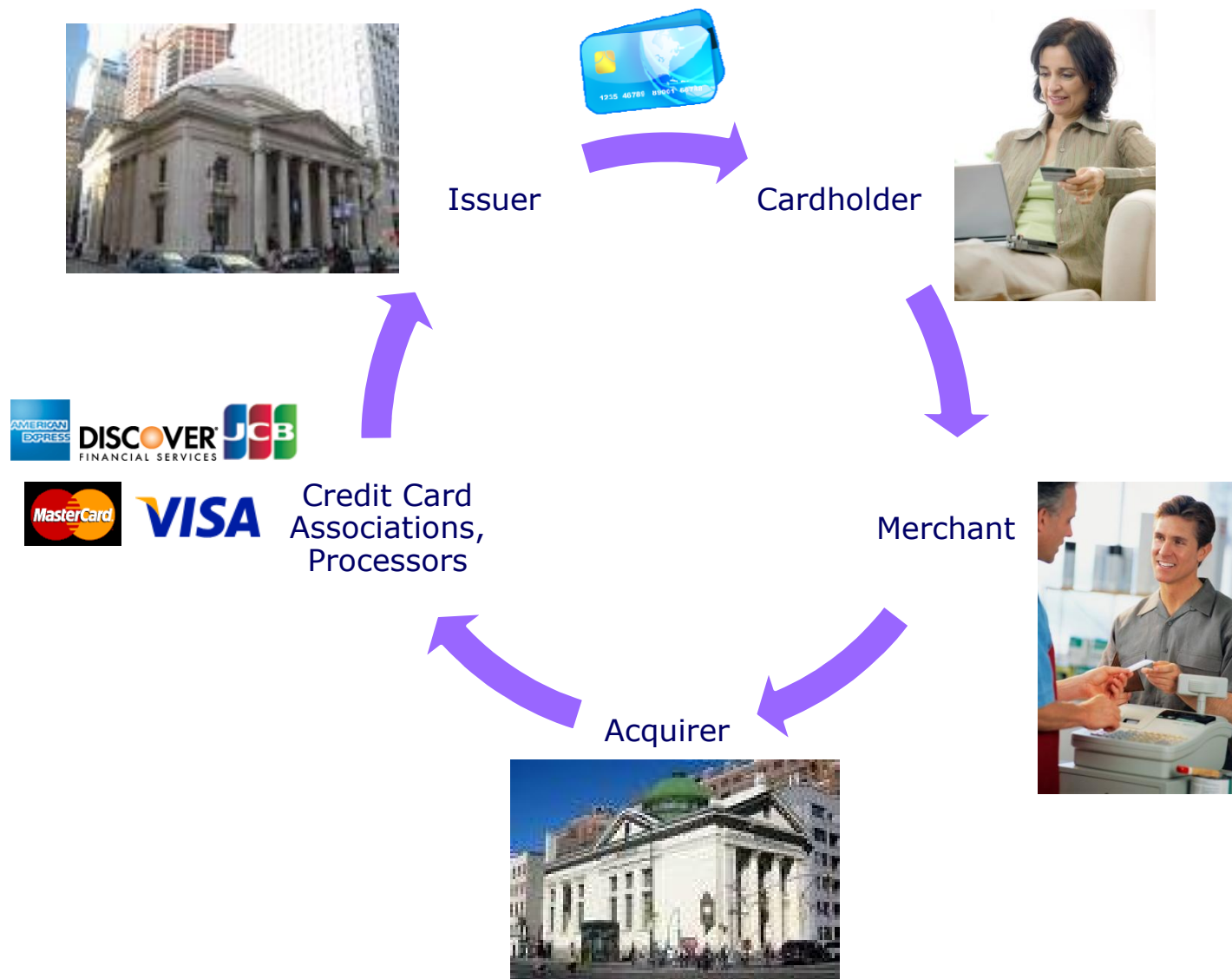
Key Roles

Parties involved in credit card transactions

Entity	Description
Issuer	<ul style="list-style-type: none"> • Financial Institution (including Banks) that issues credit cards to cardholders • Contracts with cardholder on financial terms of credit card • Maintains and manages the credit card account
Cardholder	<ul style="list-style-type: none"> • Credit card consumer • Uses credit card obtained from an Issuer for purchases • Makes payments to Issuer for credit card purchases
Merchant	<ul style="list-style-type: none"> • Business that accepts credit card payments • Brick and mortar stores, online stores, restaurants, airlines etc. • Contracts with credit card brand
Acquirer	<ul style="list-style-type: none"> • Financial Institution that acts as intermediary between merchants that accept credit card payments and the credit card Issuers • Maintains and manages merchant credit card transaction accounts • Collects payment from Issuer for credit card transactions
Service Provider (e.g., Processors)	<ul style="list-style-type: none"> • Credit card transaction processing, production and mailing of card cards, billing services, customer service support and call centers, etc.
Payment Brand (e.g., Visa, MasterCard)	<ul style="list-style-type: none"> • Processing organization that licenses Issuers to issue and merchants to accept credit cards • Serves as an intermediary between Acquirers and Issuers

Introduction to Credit Card Payments

Key Players



PCI DSS - Overview

What is the PCI DSS?

- The Payment Card Industry Data Security Standard (PCI DSS) defines a set of security requirements for the protection of credit card information.
- The initial version of the PCI DSS (version 1.0) was released in December 2004.
- The PCI DSS is maintained by the Payment Card Industry Security Standards Council (PCI SSC), and organization established by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.
- The PCI DSS is comprised of 12 requirements grouped under six goals:
 - Build and Maintain a Secure Network
 - Protect Cardholder Data
 - Maintain a Vulnerability Management Program
 - Implement Strong Access Control Measures
 - Regularly Monitor and Test Networks
 - Maintain an Information Security Policy

PCI DSS - Overview

PCI DSS Requirements:

Over 200 specific sub-requirements are included in the 12 main requirements listed below.

Build and Maintain a Secure Network

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

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

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

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

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

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

Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

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

Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

Why PCI?

Impact of Credit Card Fraud

- Payment card fraud has reached a new level of intensity and consumer awareness due to a series of significant, recent public security breaches, including:
 - In late January of 2009, **Heartland Payment Systems**, a credit card payment processor that handles 100 million transactions a month, announced what may be the biggest credit card information breach in history.
 - Compromise believed to be related to malicious software
 - In August of 2008, 11 people were arrested and charged with the theft and sale of credit and debit card information relating to over 40 million cardholders.
 - Broke into merchants' wireless networks
 - TJ Maxx, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21 and DSW
 - In March of 2008, **Hannaford Brothers Co.**, an East Coast grocery chain, announced that over 4 million credit cards were compromised.
 - Hannaford was "PCI Compliant" at time of breach
 - Hackers said to capture data transmission across private networks
 - Late 2006, a credit card compromise was discovered at **TJX (TJ Maxx)**.
 - Initial company estimates at over 45 million cards
 - Compromised over a period of more than 18 months
 - Subsequent lawsuits by banks put the estimate closer to 94 million
 - Compromise occurred due to an improperly configured wireless network

Why PCI? (cont.)

Impact of Credit Card Fraud (Cont.)

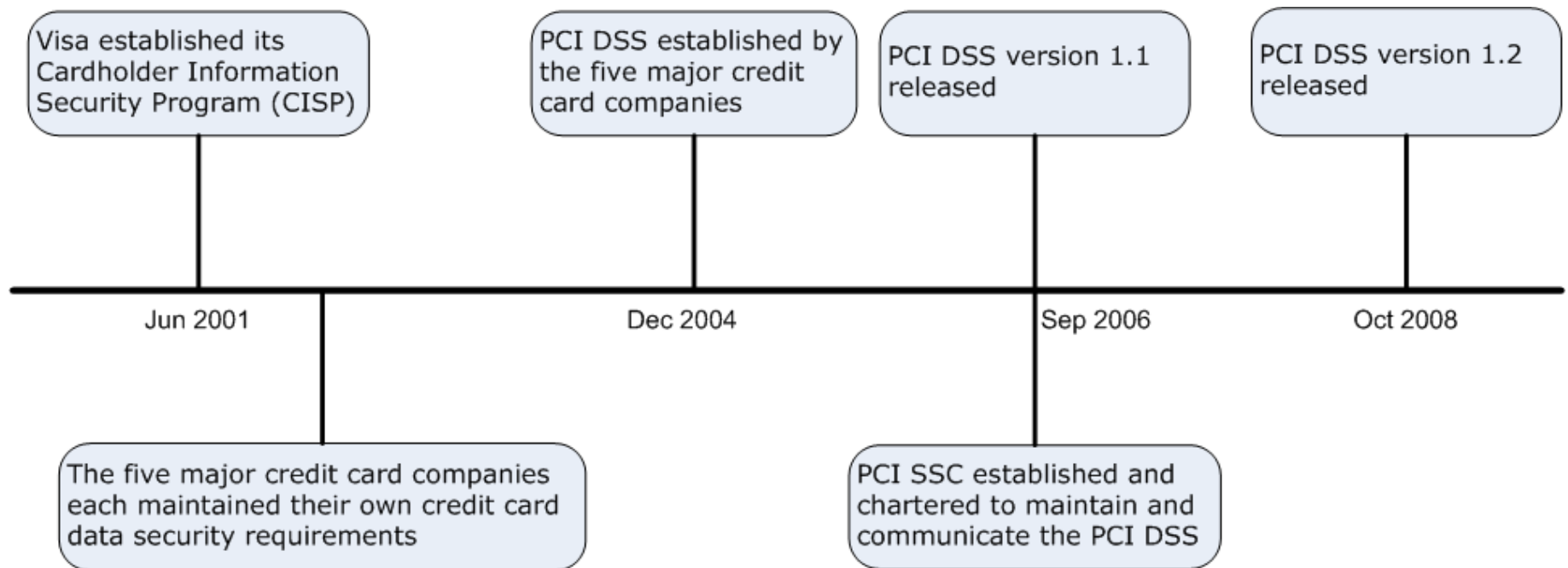
- Impacts of card breaches include, but are not limited to:
 - Significant brand impact associated with public notification of data breach
 - Fines levied by federal agencies (i.e., Federal Trade Commission)
 - Payment brand fines and dispute resolution costs
 - Litigation
 - Prevailing industry and customer perception of correlation between data breach and identity theft
- The increase in frequency and size of data breaches, as well as escalating counterfeit credit card fraud, has intensified scrutiny around how cardholder data is protected.

Focus on PCI DSS

- The PCI DSS provides prescriptive requirements that target protection of cardholder data, especially within retail environments.
- As a result, the industry presence and relevance of the PCI DSS continues to grow.
- Payment brands are also instituting more significant countermeasures to non-compliance (e.g., fines, termination of card acceptance agreements).

PCI DSS History

PCI DSS Timeline



Compliance with the PCI DSS

To whom does the PCI DSS apply?

- The PCI DSS requirements apply to all merchants and other companies that store, process or transmits credit card information.

Responsibility for compliance

- The PCI SSC maintains and administers the PCI DSS but does not enforce compliance.
- Each credit card brand (credit card company) is responsible for enforcing their PCI DSS compliance policy.
- A credit card brand may enforce compliance to their security policy (compliance to PCI DSS) on merchants, their banks (acquirers), and processors.

Different compliance validation for different classes of merchants

- Each credit card brand has different requirements for PCI DSS compliance validation, primarily based on merchant's credit card transaction volume.
- American Express, Discover, MasterCard, and Visa define merchant "Levels".
- Different compliance requirements apply to different Merchant Levels.

Merchant Levels

Merchant Level Definitions				
Payment Brand	Level 1	Level 2	Level 3	Level 4
American Express Data Security Operating Policy	<ul style="list-style-type: none"> 2.5+ million transactions per year; or Has had a data incident; or American Express identifies as Level 1 	<ul style="list-style-type: none"> 50,000 to 2.5 million transactions per year 	<ul style="list-style-type: none"> Less than 50,000 transactions per year 	N/A
Discover Financial Services DISC program	<ul style="list-style-type: none"> 6+ million transactions per year; or Level 1 merchant for another payment brand; or Discover identifies as Level 1 	<ul style="list-style-type: none"> 1 million to 6 million transactions per year; or Level 2 merchant for another payment brand 	<ul style="list-style-type: none"> 20,000 to 1 million "card-not-present" transactions per year; or Level 3 merchant for another payment brand 	<ul style="list-style-type: none"> All other merchants
MasterCard SDP program	<ul style="list-style-type: none"> 6+ million transactions per year; or Has experienced account compromise; or Level 1 merchant for another payment brand; or MasterCard identifies as Level 1 	<ul style="list-style-type: none"> 1 million to 6 million transactions per year; or Level 2 merchant for another payment brand 	<ul style="list-style-type: none"> 20,000 to 1 million e-commerce transactions per year; or Level 3 merchant for another payment brand 	<ul style="list-style-type: none"> All other merchants
Visa CISP	<ul style="list-style-type: none"> 6+ million transactions per year; or Visa identifies as Level 1 	<ul style="list-style-type: none"> 1 million to 6 million transactions per year 	<ul style="list-style-type: none"> 20,000 to 1 million e-commerce transactions per year 	<ul style="list-style-type: none"> Less than 20,000 e-commerce transactions per year Other merchants up to 1 million transactions per year

PCI Compliance

Compliance with the PCI DSS

- PCI compliance is required by all entities that store, process or transmit cardholder information.
- In order to be considered "PCI compliant", an entity must comply with all of the requirements in the PCI DSS (either directly or through appropriate compensating controls).
- Compliance validation requirements vary depending on the payment brand program and the merchant or service provider level (e.g., Level 1 through 4).
- An entity may be able to assess compliance with the PCI DSS through a singular review; however, the entity would still be required to follow each payment brand's respective compliance validation and reporting requirements.
- Non compliance can result in fines levied by credit card companies against merchants, processors and acquiring banks.

Compliance Validations

Different forms of PCI DSS compliance validation based on Merchant Level

- Possible forms of validations include:
 - Annual Report on Compliance ("ROC") by a Qualified Security Assessor ("QSA") or a compliance report by the merchant's Internal Audit function, provided that a letter signed by a merchant officer accompanies the report and is accepted by the merchant's Acquirer
 - Network security scan by an Approved Scan Vendor ("ASV")
 - Annual Self-Assessment Questionnaire ("SAQ") by the merchant
- A QSA is a vendor qualified by the PCI SSC to perform PCI DSS compliance assessments.
- As of PCI DSS version 1.2, a merchant's Internal Audit function was included within the definition of "assessor" as an alternative to QSAs.
- An ASV is a vendor qualified by the PCI SSC to perform PCI DSS related network vulnerability scans
- Each credit card brand outlines its own requirement for each merchant level (typically some combination of a compliance report, network scan, or SAQ).

Compliance Validation Requirements

Compliance Validation Requirements for Defined Merchant Levels				
Payment Brand	Level 1	Level 2	Level 3	Level 4
American Express	<ul style="list-style-type: none"> Annual Onsite Security Assessment Report, and Quarterly Network Scan 	<ul style="list-style-type: none"> Quarterly Network Scan 	<ul style="list-style-type: none"> Quarterly Network Scan 	N/A
Discover Financial Services	Discover Financial Services introduced merchant levels on January 16, 2009.			
MasterCard	<ul style="list-style-type: none"> Annual ROC by a QSA or compliance report by merchant's Internal Audit Quarterly network scan by ASV 	<ul style="list-style-type: none"> Annual SAQ Quarterly network scan by ASV 	<ul style="list-style-type: none"> Annual SAQ Quarterly network scan by ASV 	<ul style="list-style-type: none"> Annual SAQ Quarterly network scan by ASV Compliance validation requirements set by acquirer
Visa	<ul style="list-style-type: none"> Annual ROC by a QSA or compliance report by merchant's Internal Audit Quarterly network scan by ASV Attestation of Compliance Form 	<ul style="list-style-type: none"> Annual SAQ Quarterly network scan by ASV Attestation of Compliance Form 	<ul style="list-style-type: none"> Annual SAQ Quarterly network scan by ASV Attestation of Compliance Form 	<ul style="list-style-type: none"> Annual SAQ recommended Quarterly network scan by ASV, if applicable Compliance validation requirements set by acquirer

Internal Audit's Role

Merchant Compliance to PCI DSS

- Internal Audit may perform PCI DSS compliance assessments as of Version 1.2 of the PCI DSS
 - Understand the PCI DSS requirements and have sufficient technical knowledge in the security domains covered by the PCI DSS
 - Understand the merchant's business processes and data flows related to credit card information
- Internal Audit may also provide guidance on the PCI DSS (whether or not they are acting as the compliance assessor)
 - Identify systems and processes that may be required to undergo PCI DSS assessments
 - Advise on PCI DSS requirements and provide support in interpreting requirements
 - Participate in the remediation of gaps identified during an assessment
 - Be involved in the SAQ process
 - Evaluate effectiveness of the PCI DSS compliance program
 - Help identify compensating controls, determine level of risk for gaps
 - Be involved in compliance reporting to the merchant's acquiring bank

Internal Audit's Role

Processor Compliance to PCI DSS

- Credit card brands have compliance requirements for processors
 - American Express requires an on-site review and a network scan by an ASV
 - Discover provides processors with an option to perform an on-site review or SAQ
 - Visa and MasterCard uses Service Provider Level definitions (Level 1 and Level 2 Processors) based on the number of transactions processed
 - Compliance requirements consist of an on-site review by a QSA or SAQ based on Processor Level classification
 - Network scan by an ASV is required
- Current language specifically refers to QSAs for on-site review for processors
- Internal Audit may assist with internal efforts and guidance on PCI DSS, as previously described for merchants

Internal Audit's Role Acquiring Banks

- Credit card brands each have their own requirements for PCI DSS compliance for Acquiring banks.
 - Discover requires its acquiring banks to report both on their own compliance to PCI DSS (as a provider) and the compliance status of their merchants
 - Visa and MasterCard do not require PCI DSS compliance by banks; however, they do require acquiring banks to report on the compliance status of their merchants (fines may be imposed for failure to manage and report compliance to PCI DSS by their merchants)
- Internal Audit may consider providing guidance on PCI DSS to banks
 - Advise on PCI DSS requirements and provide support in interpreting requirements
 - Evaluate effectiveness the PCI DSS merchant compliance monitoring program
 - Support PCI DSS compliance reporting (of merchants and/or acquirer) to credit card brands

PCI Challenges

- Identifying and understanding cardholder data inventory (i.e., the “PCI compliance footprint”)
- Defining appropriate strategies to remediate issues of non-compliance
 - Common issues of non-compliance often exist at the system infrastructure level (e.g., lack of encryption, network segmentation, etc.) and can require a significant effort to remediate.
 - Defining and implementing viable compensating controls (when traditional controls cannot be implemented) in order to overcome inadequacies due to legacy infrastructure, application limitations etc.
 - Highly heterogeneous network, server, operating system infrastructure adds to the complexity level.
- Concurrently addressing compliance with the increasing number of security requirements:
 - Regulatory: Gramm-Leach-Bliley Act (GLBA), California Security Breach Information Act (SB-1386), European Union (EU) Data Directive, Sarbanes-Oxley, Health Insurance Portability and Accountability Act (HIPAA), etc.
 - Contractual: Contractual obligations with business partners, service providers, outsourcing, etc.

Common Compliance Issues

Areas we have commonly seen compliance issues include:

- Sensitive authentication data is stored (PCI DSS Requirement 3.2).
 - The PCI DSS explicitly prohibits storage of magnetic stripe data (i.e., authentication or “prohibited” data) post authorization (even if encrypted).
 - Merchants often must upgrade or replace POS systems, which may store sensitive authentication data by default.
- Cardholder data is not encrypted (PCI DSS Requirement 3.4).
 - If Requirement 3.4 cannot be met, acceptable compensating controls may be considered. PCI DSS outlines requirements for compensating controls (Appendix B of the PCI DSS)
- Wireless networks are not secured (PCI DSS Requirement 2.1.1).
 - Weaknesses in wireless networks proved to be costly to merchants (e.g., TJ Maxx).
- Access to cardholder data is not logged and/or monitored (PCI DSS Requirement 10).
 - Logs may be critical to investigate current or past security incidents.
- Insufficient system hardening (PCI DSS Requirement 2.2).
- Insufficient patching process (PCI DSS Requirement 6.1).
- Security practices are not integrated into custom code development (PCI DSS Requirement 6.3) and web application development (PCI DSS Requirement 6.5)

Compensating Controls

- The PCI DSS allows for compensating controls "...when an entity cannot meet a technical specification of a requirement, but has significantly mitigated the associated risk."
- Compensating controls must:
 1. Meet the intent and rigor of the original stated PCI DSS requirement
 2. Repel a compromise attempt with similar force
 3. Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements) and
 4. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement
- Compensating controls may be considered for all requirements EXCEPT storage of prohibited data (i.e., full track data, CVV2, PIN) post-authorization (Requirement 3.2).

References

PCI DSS Council:

Overview: <https://www.pcisecuritystandards.org/tech/index.htm>

Glossary of Terms: <https://www.pcisecuritystandards.org/tech/glossary.htm>

Qualified Security Assessors (QSAs):
https://www.pcisecuritystandards.org/resources/qualified_security_assessors.htm

Approved Scanning Vendors (ASVs):
https://www.pcisecuritystandards.org/resources/approved_scanning_vendors.htm

Compliance Requirements:

"American Express Data Security Operating Policy for U.S. Merchants"
https://www209.americanexpress.com/merchant/singlevoice/pdfs/en_US/DSOP_Merchant_US.pdf

"Discover Announces PCI Data Security Merchant Levels"

<http://investorrelations.discoverfinancial.com/phoenix.zhtml?c=204177&p=irol-pressArticle&ID=1245496&highlight=>

JCB Data Security Program

<http://www.jcb-global.com/english/jdsp/index.html>

"Merchant Levels Defined"

http://www.mastercard.com/us/sdp/merchants/merchant_levels.html

"Visa Sets Global PCI DSS Deadlines"

<http://www.corporate.visa.com/md/nr/press873.jsp>

Review of Today's Discussion

- Introduction to Credit Card Payments
- PCI DSS
- Compliance Validation
- Internal Audit's Role
- Challenges and Common Compliance Issues

For More Information

Carey Carpenter
Senior Manager
Deloitte & Touche LLP
ccarpenter@deloitte.com
808-543-0776

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.