



January 31, 2014

11:30am – 12:30pm  
Central

Hosted by:  
Texas.gov

Presented by:  
Jayne Holland  
Barbara Brinson

# Payment Card Industry Compliance Overview

## Securing Government Payments

Audio Dial In: 866-740-1260 Passcode: 2345957

# **Purpose of Payment Card Industry Data Security Standards (PCI-DSS)**

- **Set of global security standards and best practices**
- **Applies to merchants, processors, acquirers, issuers, providers and those who store, process and transmit cardholder data**
- **Comprises minimum set of requirements**
- **Developed by the Payment Card Industry Security Standards Council (“the Council”) who is responsible for development, management, education and awareness of the PCI-DSS**

# Suite of Standards Managed by PCI-SSC

- **PCI-PTS: Manufacturers of PIN Entry Devices**
- **PCI PA-DSS: Software developers and covers payment applications**
- **PCI-DSS: Merchants and service providers to address secure payment processing environments**
  - ✓ Most significant
  - ✓ In depth security strategy
  - ✓ Targets different levels of your infrastructure

## Protection of Cardholder Payment Data



# What does PCI-DSS cover?

## ■ **Security of the environment:**

- ✓ System components included in or connected to a merchant or service provider's cardholder data environment
- ✓ Any environment that receives account data from payment applications and other sources



# Securing Account Data

## ■ **Cardholder Data includes:**

- ✓ Primary Account Number (PAN)
- ✓ Cardholder Name
- ✓ Expiration Date
- ✓ Service Code

## ■ **Sensitive Authentication Data:**

- ✓ Full Magnetic strip data or equivalent on a chip
- ✓ CAV2/CVC2/CVV2/CID
- ✓ PINS/PIN blocks

# PCI-DSS Administration and Enforcement

- **American Express: Data Security Operating Policy (DSOP)**
- **Discover: Discover Information Security Compliance (DISC)**
- **JCB: Data Security Program**
- **MasterCard: Site Data Protection (SDP)**
- **Visa Inc.: Cardholder Information Security Program (CISP)**
- **Visa Europe: Account Information Security (AIS) Program**



## Responsibilities of the PCI Security Standards Council

- **Manage the security standards**
- **Define and implement validation requirements**
- **Approve companies and employees to perform assessments**
- **Maintain lists:**
  - ✓ **QSA, PA-QSA and ASV**
  - ✓ **Validated payment applications**
  - ✓ **Approved PIN transaction devices**
  - ✓ **Validated Point to Point Encryption Solutions**
- **Review selected reports**
- **Provide training to QSA, PA-QSA and ISAs**
- **Offer guidance on technologies**
- **Promote PCI security globally**

### Acronyms

QSA:	Qualified Security Assessor
PA-QSA:	Payment Application Qualified Security Assessor
ASV:	Approved Scanning Vendor
ISA:	Internal Security Assessor

## Responsibilities of Payment Card Brands

- **Develop & enforce compliance programs**
- **Assess fines or penalties for non-compliance**
- **Endorse QSA, PA-QSA and ASV company qualification criteria**
- **Accept validation documentation from approved companies**
- **Provide feedback to the Council on performance**
- **Perform forensic investigations**

### Acronyms

QSA:	Qualified Security Analyst
PA-QSA:	Payment Application Qualified Security Assessor
ASV:	Approved Scanning Vendor

## **Responsibilities of Acquirers**

- **Ensure merchants understand requirements and track compliance efforts**
- **Manage communications about PCI**
- **Working with merchants to achieve compliance**
- **Report compliance to payment brands**
- **Liability for non-compliance**

# Time Frame

## 36 Month Lifecycle - 8 stages



# What changes were made to the PCI-DSS Standard?

*Version #3  
November 2013*

## ■ **Clarifications**

- ✓ Clarified the intent of a requirement

## ■ **Additional Guidance**

- ✓ Explanation, definition or instruction to increase understanding

## ■ **Evolving Requirement**

- ✓ Ensuring standards and up to date with emerging threats and changes

# Any significant changes to Version #3?

*Effective Jan2014  
Enforcement Jan 2015*

## ■ **Penetration Testing**

- ✓ Formal pen testing methodology
- ✓ 12 months threats and vulnerabilities
- ✓ Exploitable vulnerabilities remediated and retested
- ✓ Operational effectiveness of controls if CDE is separated from other networks

## ■ **Cardholder Data Flow**

- ✓ Shared Responsibility between 3<sup>rd</sup> parties, banks, merchants, businesses, retailers and other entities
- ✓ Document requirements and responsibilities

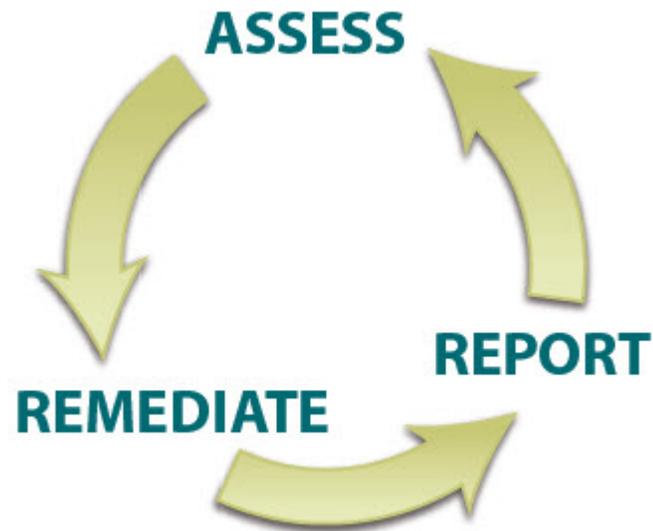
## ■ **POS Devices**

- ✓ Physical security of the devices
- ✓ Restricting access
- ✓ Detect/Report tampering

# Is Government Responsible for PCI?

- **Impossible to completely outsource PCI**
- **Need to evaluate how you receive or transmit card information in connection with what is being outsourced**

# What does PCI-DSS require you to do?



- **Assess: Identify data, take inventory and analyze**
- **Remediate: Fix vulnerabilities**
- **Report: Submit records and reports**

# Achieving PCI-DSS Compliance

- **12 general requirements and 6 milestones**
- **Continuous process**
- **Fix Vulnerabilities**
- **Merchant and Service Provider reporting to acquiring banks and card brands**
- **Assess, Remediate and Report**
- **Adhering to PCI-DSS Requirements**
- **Operationally playing your role**

# How do you demonstrate you are compliant?

*Depends on how the payment brands define Merchants and Service Level Providers*

## ■ Annual On-Site Audit

- ✓ 3<sup>rd</sup> party review by Qualified Security Assessor (QSA) utilizing PCI Security Audit Procedures and compliance report filing

## ■ Annual Self-Assessment

- ✓ Internal questionnaire based on the requirements in the PCI-DSS

## ■ Quarterly Security Scan

- ✓ 3<sup>rd</sup> Party Approved Scanning Vendor (ASV) performs non-intrusive network scan of Internet-facing perimeter systems

***\*\*Note: Only the Merchant of Record is required to demonstrate PCI Compliance.***

# Consequences of Failing to Comply

## ■ **Fines, Penalties and Other Costs**

- ✓ Varies by card brand
- ✓ Government fines
- ✓ Forensic investigation costs
- ✓ Cancelled accounts
- ✓ Breach notification costs
- ✓ Insurance claims
- ✓ Defense costs

## ■ **Reputation**

- ✓ Loss of Trust and Confidence
- ✓ Loss of relationships

## ■ **Acquirer incurs liability**

- ✓ Merchant non compliance
- ✓ Fines are passed down

# Government's Challenge

## Where do you start?

### ■ **PCI SCC Prioritized Approach Document**

- ✓ Helps expedite
- ✓ Demonstrate compliance progress
- ✓ Roadmap to address risks
- ✓ Quick Wins
- ✓ Support with financial and operational planning
- ✓ Objective and measurable progress
- ✓ Consistency with Assessors

# Recommendations for reviewing PCI-DSS

- **Assess:**
  - ✓ Identify data flow
  - ✓ Identify cardholder data
- **Remediate:**
  - ✓ Fix Vulnerabilities
  - ✓ Don't store cardholder data
- **Report**
  - ✓ Remediation validation
  - ✓ Compliance reports to banks and cards brands

# PCI-DSS Additional Information

- **PCI SSC Website**

[www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

- **Website includes the following resources:**

- ✓ PCI Standards and Supporting Documents
- ✓ FAQs, Training Information, News & Events

# Questions?

**Jayne Friedland Holland**

**913-754-7005**

**[www.egov.com](http://www.egov.com)**

**[jayne@egov.com](mailto:jayne@egov.com)**

