

PCI DSS 3.2

Speaker Name: Pramod Deshmane, *SVP ControlCase*



Agenda

- **PCI DSS Background**
- **PCI DSS Best Practices Becoming Mandatory**
- **Q&A**

PCI DSS – Historical Perspective

- Different Card Brands (Visa, MasterCard, Amex, Discover, JCB)
- Different Compliance Requirements
- Year 2006 – Formation PCI SSC



What is PCI DSS Standard

- ❑ Data Security Standard adopted by major card processing networks (Visa, MasterCard, etc.) to combat fraud and promote secure processing of payment card transactions
- ❑ Unified standard for security associated with card data storage, transmission, and processing
- ❑ PCI DSS Compliance is recommended / mandatory as per the organizations levels that deals with card data.

PCI Family of Standards

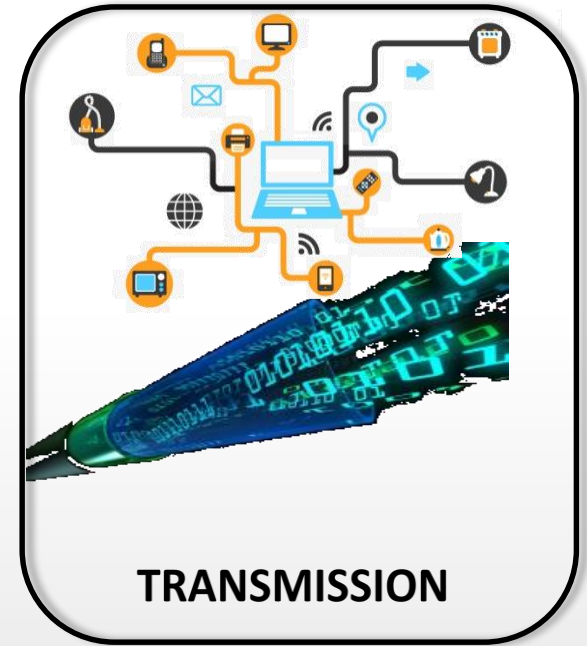
Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users

PCI DSS Applicability

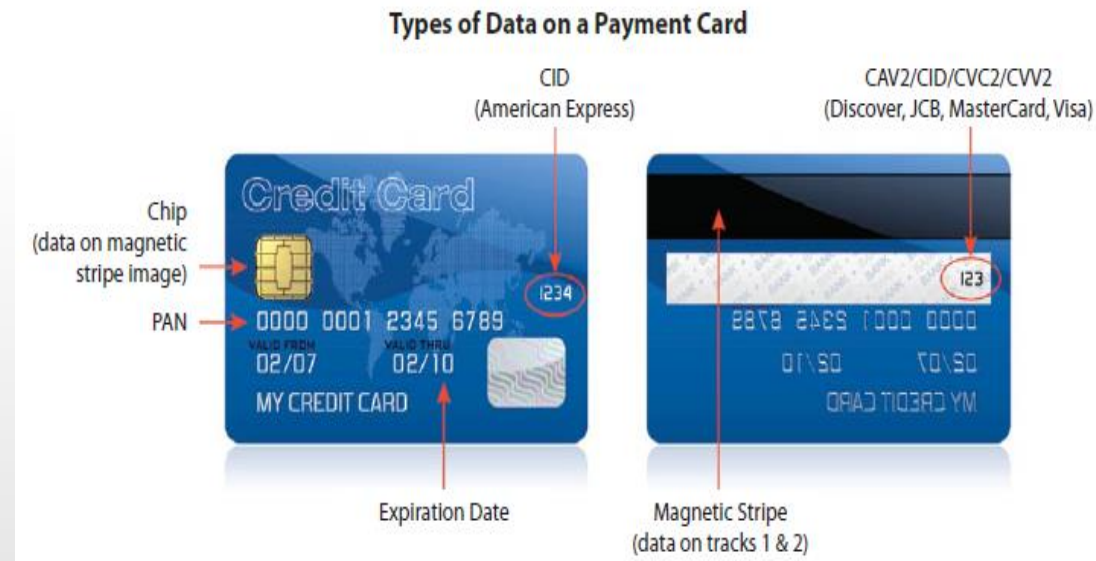
All entities that **STORE**, **PROCESS**, **TRANSMIT** Cardholder Data and service providers who manages the system components, where there may be an **impact on the security** of the cardholder data environment.



Managed Services and connected entities impacting CHD

Data in Question (Credit & Debit Card)

- Cardholder number (Called PAN)
- Cardholder Name
- Expiration Date
- Service Code
- CVV/CVV2/CVC2
- Track Data
- PIN



PCI Requirements

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect cardholder data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored cardholder data4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Use and regularly update anti-virus software or programs6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to cardholder data by business need-to-know8. Assign a unique ID to each person with computer access9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security for employees and contractors



PCI DSS Best Practices Becoming Mandatory

PCI DSS Best Practices Becoming Mandatory

- PCI DSS v3.2 was released in April 2016
- PCI DSS v3.2 became effective from November 2016
- Changes in PCI DSS v3.2 were categorized in three types
 - Clarification
 - Additional Guidance
 - Evolving requirements
- Evolving requirements (Best Practices) will be mandatory from **Feb 1st 2018**

Req. 3.5.1 - Cryptographic Architecture Documentation

Applicability - Service Provider

(Effective February 1, 2018)

To maintain a documented description of the cryptographic architecture

- *Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date*
- *Description of the key usage for each key*
- *Inventory of any HSMs and other SCDs used for key management*

How to comply:

- Maintain a documentation on your cryptographic architecture explaining the types of encryption algorithms in use, the key strength and expiry
- Inventory document to include *HSMs and other SCDs used for key management if in use*

Req. 6.4.6 – PCI controls verification after changes

Applicability - Service Provider / Merchant

(Effective February 1, 2018)

Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.

- *Having processes to analyse significant changes helps ensure that all appropriate PCI DSS controls are applied to any systems or networks added or changed within the in-scope environment*
- *Building this validation into change management processes helps ensure that device inventories and configuration standards are kept up to date and security controls are applied where needed*
- *A change management process should include supporting evidence that PCI DSS requirements are implemented or preserved through the iterative process.*

How to comply:

- Create a checklist or add the list for PCI controls for verification in change management process to ensure all the applicable controls are verified before the change is closed

Req. 8.3, 8.3.1 – Multi-factor authentication for CDE access

Applicability - Service Provider / Merchant

(Effective February 1, 2018)

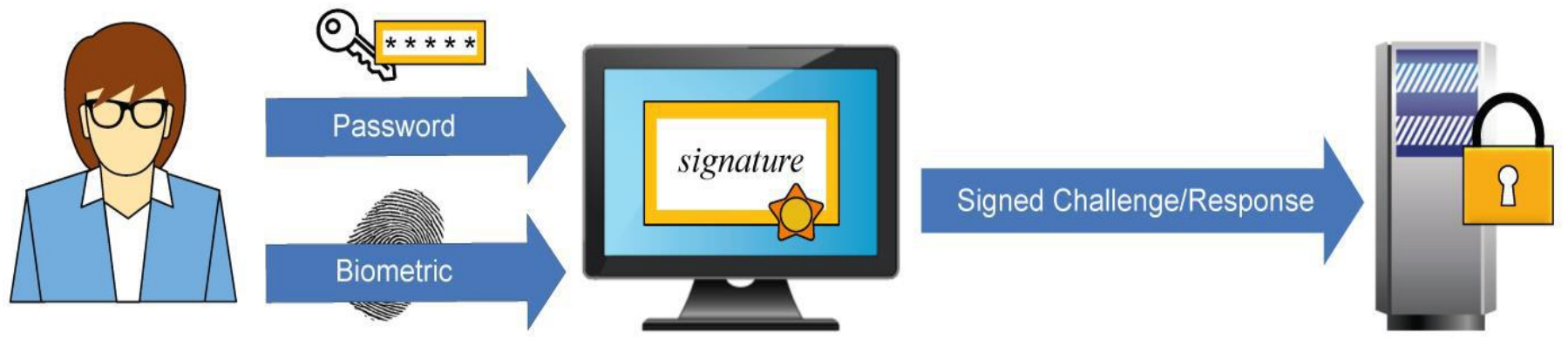
Incorporate multi-factor authentication for all personnel with non-console administrative access to the CDE

- *This requirement is intended to apply to all personnel with administrative access to the CDE*
- *This requirement applies only to personnel with administrative access and only for non-console access to the CDE; it does not apply to application or system accounts performing automated functions*
- *Multi-step vs. Multi-factor*

How to comply:

- You can implement Multi-factor authentication at network level or while logging to system / application itself, also if use MFA to authenticate at network level then you don't need MFA again for access to System
- Multi-factor authentication through Jump-box used for CDE access

Multi-Factor Authentication



Req. 10.8,10.8.1 – Logging Critical security control systems failure

Applicability - Service Provider

(Effective February 1, 2018)

Service providers to detect and report on failures of critical security control systems

- *Implement process to Detect, Alert and Respond to Security control failures effectively*
- *If critical security control failures alerts are not quickly and effectively responded to, attackers may use this time to insert malicious software, gain control of a system, or steal data from the entity's environment*

How to comply:

- Identify the critical security controls systems
- Implement the monitoring and timely alerting mechanism to notify system failure
- Define the procedures on how to respond to critical security controls failure

Req. 11.3.4.1 – Segmentation testing

Applicability - Service Provider

(Effective February 1, 2018)

Service providers to perform penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods

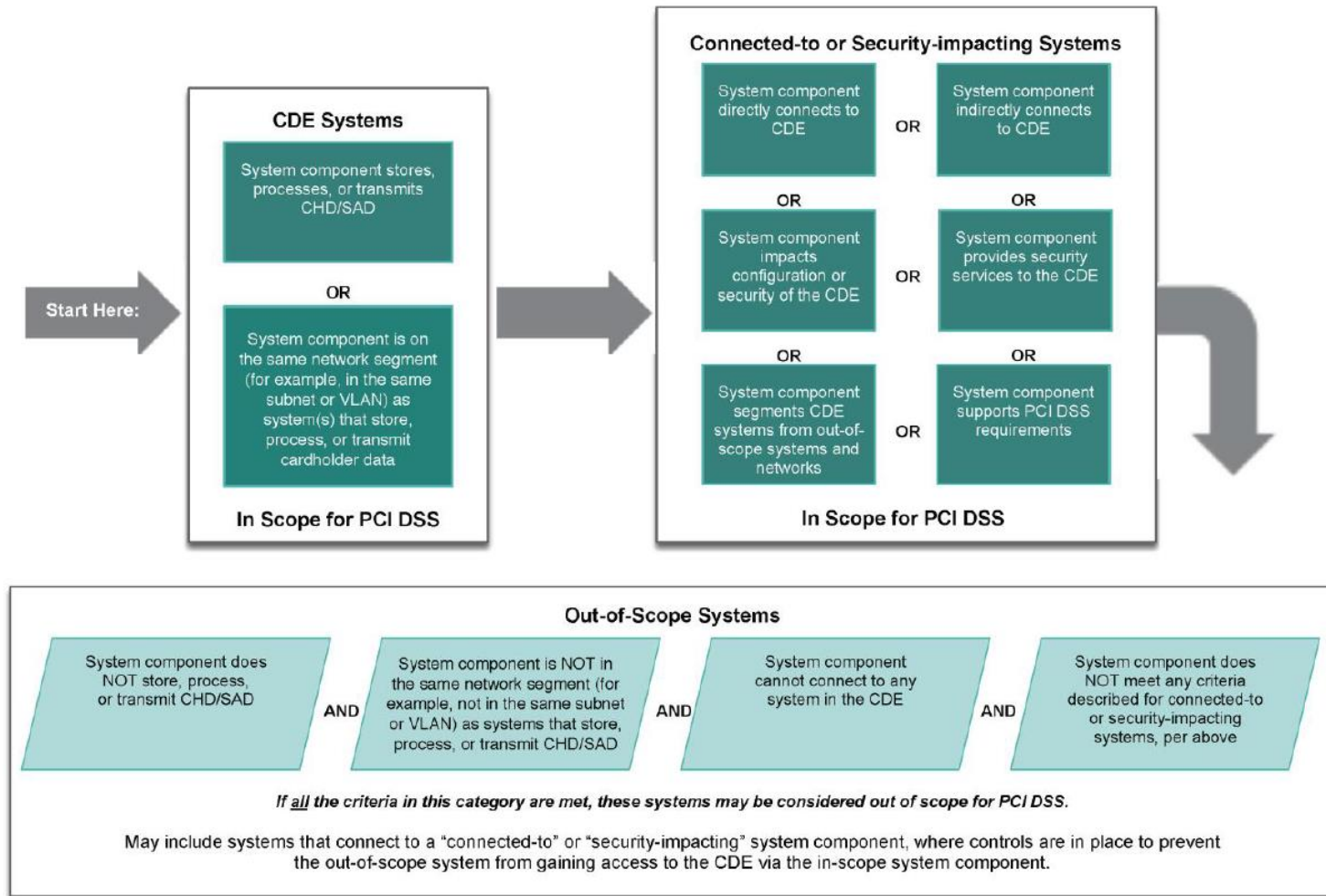
- *Validation of PCI DSS scope should be performed as frequently as possible to ensure PCI DSS scope remains up to date and aligned with changing business objectives*
- *The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE*

How to comply:

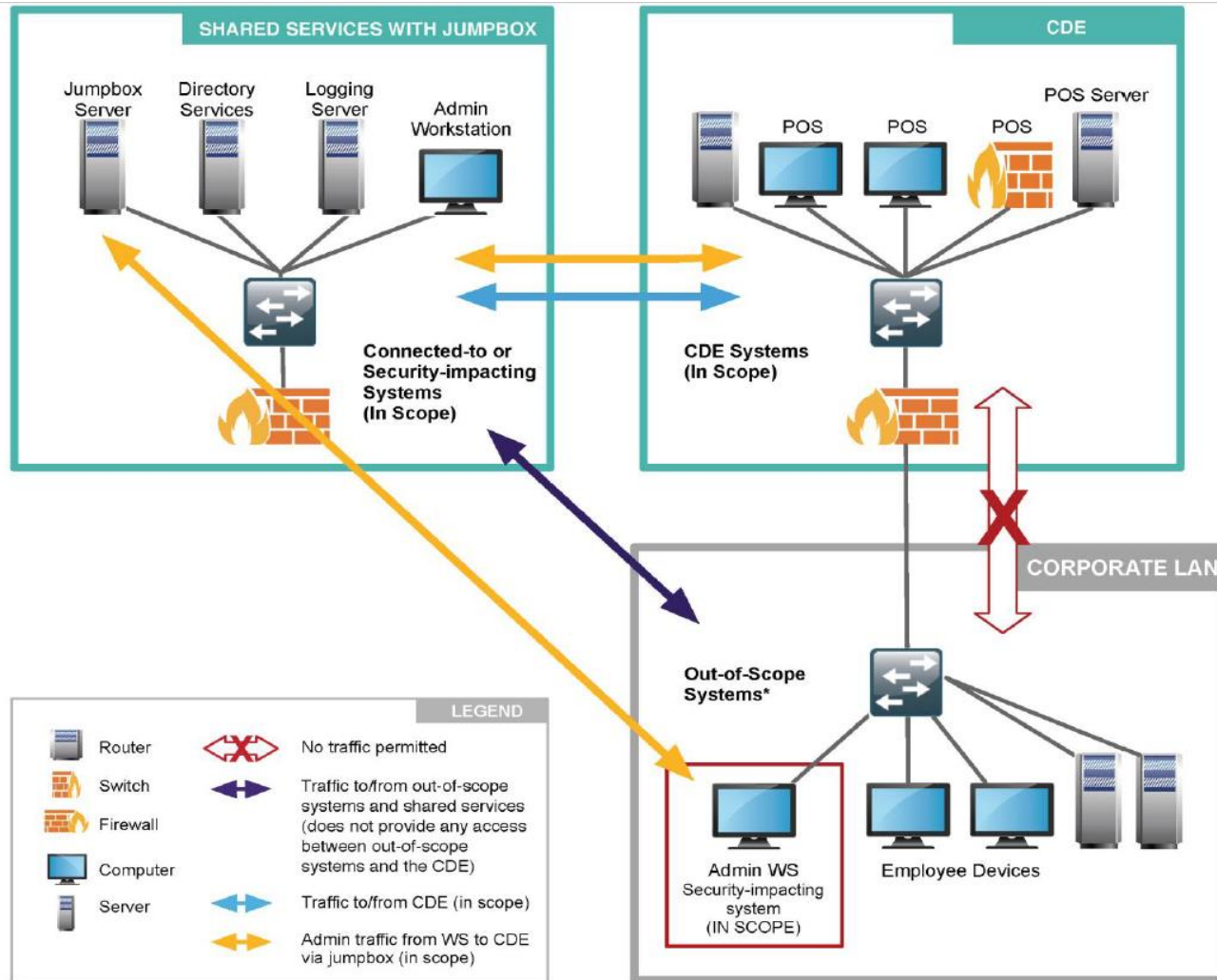
- Document your in-scope and out of scope segments and perform the segmentation test at-least every six months
- Add this as a control as part of your change management process to support Req. 6.4.6

PCI Segmentation

FIGURE 1 – PCI DSS Scoping Categories



PCI Segmentation



Req. 12.4.1 - Establish responsibilities for executive management

Applicability - Service Provider

(Effective February 1, 2018)

Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program

- *Executive management should assign overall responsibility of PCI DSS compliance program*
- *Defining a charter which outlines the conditions under which PCI DSS compliance program is organized and communicated to Executive management*

How to comply:

- Identify the executive management team for PCI DSS compliance program
- Ensure that executive management is made well aware of the actual compliance process and plans on regular basis so that they have complete visibility in to PCI DSS program

Req. 12.11, 12.11.1 – Review for security policies and operational procedures

Applicability - Service Provider

(Effective February 1, 2018)

Service providers to perform reviews at least quarterly, to confirm personnel are following security policies and operational procedures.

- *Perform at least quarterly reviews to confirm the personnel are following operational procedures to confirm that personnel are following security policies and operational procedures to check effectiveness of controls and working as intended.*
 - *Daily log reviews*
 - *Firewall rule-set reviews*
 - *Applying configuration standards to new systems*
 - *Responding to security alerts*
 - *Change management processes*

How to comply:

- Define the process for measuring the effectiveness of controls
- Maintain a quarterly review documentation to show how the effectiveness of controls

Req. 2.2.3, 2.3, 4.1– Migration from SSL and TLS 1.0

Applicability - Service Provider/Merchant

(Effective July 1, 2018)

All entities should migrate from SSL / early TLS version to TLS secure version

- *Encrypt all non-console administrative access using strong cryptography.*
- *Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.*

How to comply:

- Ensure all system platforms / applications are configured to only use TLS 1.1 or preferably TLS 1.2 protocol prior to June 30, 2018


Questions And Answers

Thank You

Pramod Deshmane

Sr. Vice President – Certifications

 pdeshmane@controlcase.com

 +1 571 422 7018