Payment Card Industry Data Security Standards

Christopher Kennedy

Presentation Updated 2015-04-10

NSU NOVA SOUTHEASTERN UNIVERSITY
Office of Innovation and Information Technology

70 Million Credit Card Number Stolen

56 Million Credit Card Numbers Stolen

Heartland PAYMENT SYSTEMS™

The Highest Standards | The Most Trusted Transactions

130 Million Credit Card Numbers Stolen

Payment Card Industry Data Security Standard (PCI DSS)

- Security Standards for Organizations that Handle Branded Credit Cards from the major issuers – MasterCard, Visa, Discover, Amex and JCB
- Standards created to increase controls around cardholder data and reduce credit card fraud
- Originally 5 separate programs
- Formed Payment Card Security Standards Council
- PCI DSS v 1.0 Released in December 2004

Who Must Comply?

- Anyone Collecting Card Holder Data
- Regardless of Size

PCI Data Security Standard – High Level Overview

Build & Maintain a Secure Network and Systems	• Install and maintain a firewall configuration to protect cardholder data • Do not use vendor supplied defaults for system passwords and other security
Protect Cardholder Data	• Protect stored cardholder data • Encrypt transmission of cardholder data across open public networks.
Maintain a Vulnerability Management Program	• Protect all systems against malware and regularly update anti-virus software or programs • Develop and Maintain secure systems and applications
Implement Strong Access Control Measures	• Restrict access to cardholder data by business need to know • Identify and authenticate access to system components • Restrict physical access to cardholder data
Regularly Monitor and Test Networks	• Track and monitor all access to network resources and cardholder data • Regularly test security systems and processes
Maintain an Information Security Policy	• Maintain a policy that addresses information security for all personnel.

Cardholder Data

Account Data	
Cardholder Data	**Sensitive Authentication Data**
* Primary Account Number * Cardholder Name * Expiration Date * Service Code	* Full Track Data (magnetic-stripe data or equivalent on chip) * CAV2/CVC2/CVV2/CID * Pin's / Pin Blocks

- PAN - Full account number of card
- Cardholder Name - how it reads on the card
- Expiration Date
- Service Code - 3 or 4 digits on magnetic strip that specifies the acceptance requirement
- Full Track Data - Data on the magnetic strip
- CVC - calculated through a specific algorithm using number of items about the account
- PIN - generated by cardholder (ex - ATM cash advance)

Storage of Cardholder Information

		Data Element	Storage Permitted	Render Stored Data Unreadable per Requirement 3.4
Account Data	Cardholder Data	Primary Account Number (PAN)	Yes	Yes
		Cardholder Name	Yes	No
		Service Code	Yes	No
		Expiration Date	Yes	No
	Sensitive Authentication Data	Full Track Data	No	Cannot Store per Requirement 3.2
		CAV2/CVC2/CVV2/CID	No	Cannot Store per Requirement 3.3
		PIN/PIN Block	No	Cannot Store per Requirement 3.4

- PCI DSS Requirements 3.3 and 3.4 apply only to PAN. If PAN is stored with other elements of cardholder data, only the PAN must be rendered unreadable according to PCI DSS Requirement 3.4.
- Sensitive authentication data must not be stored after authorization, even if encrypted.

Common Myths of PCI DSS

Myth – Outsourcing card processing makes NSU compliant.

Outsourcing simplifies payment card processing but does not provide automatic compliance. NSU must protect cardholder data when received, process charge backs and refund.

Common Myths of PCI DSS

Myth – PCI Compliance is an OIIT project.

The OIIT staff implements technical aspects of PCI related systems , but compliance is more than a “project” with a beginning and end –its an ongoing process of assessment, remediation and reporting. PCI compliance is a business issue that is best addressed by a multi-disciplinary team.

Common Myths of PCI DSS

Myth – PCI will make us secure.

Completion of a system scan or assessment for PCI is a snapshot in time.

Common Myths of PCI DSS

Myth – PCI is unreasonable; it requires too much.

Most aspects of the PCI DSS are already a common best practice for security. The standards provide significant detail, which benefits merchants and processors by not leaving them to wonder “Where do I go from here?”

Cost of Non-Compliance

- Fines and Penalties
- Card Reissuing Costs
- Loss of Card Processing Privileges
- Reputational Risk

Best Practices

- Lock your computer screen and terminal
- Lock your desk / drawer / office
- Do not write down credit card Sensitive Authentication Data
- Do not share login information
- Do not use memory sticks on NSU devices
- Do not send credit card information via interoffice mail

How to practice PCI Compliance

- Take the Blackboard training course: DSS End-User Course **annually.**

  - To complete the Blackboard training you must be setup in the course first.
  - To get set up, email pci@nova.edu including your name and email address. You will get an email back explaining how to access and complete the training.

- Attend in-house seminars **annually.**

Additional Resources

- NSU PCI Policies located at http://www.nova.edu/treasury/forms/index.html
  - NSU PCI General Policy
  - NSU PCI Data Retention and Disposal Policy
  - NSU Guidelines and Procedures
- PCI Security Standards https://www.pcisecuritystandards.org/index.php
- Specific Questions – pci@nova.edu