CUNA
TECHNOLOGY COUNCIL

PCI-DSS for Credit Unions

Tom Schauer; CEO @ TrustCC

CISSP, CISA, CISM, CRiSC, CEH, CTGA

tschauer@trustcc.com

TRUSTCC™

Devoted to Banking, Tecnically Superior, Trusted™

CUNA TECHNOLOGY COUNCIL

Misinformation

- Opinion: There is more confusion and more misinformation about PCI requirements than any other standard…

- Expectations by card brands are poorly communicated for all roles other than “merchant”.

TRUST-CC™

Devoted to Banking, Tecnically Superior, Trusted™

CUNA TECHNOLOGY COUNCIL

PCI-DSS Version 3

- The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that **ALL** companies that **process, store** or **transmit** credit card information maintain a secure environment.
- PCI-PIN is a separate standard focused specifically on the security of PIN based transaction.

TRUST-CC™

Devoted to Banking, Tecnically Superior, Trusted™

CUNA TECHNOLOGY COUNCIL

Roles

- Issuer – Financial Institution offering the Card
- Acquirer or Acquiring Bank – Acquire transactions on behalf of a merchant
- Merchant – Accepts Card Data for a Transaction
- Processor – Processes card data

- Most CUs are issuers and merchants (acquirer). Most outsource processing to a third party.

TRUST-CC™

Devoted to Banking, Tecnically Superior, Trusted™

- **Q: Do organizations using third-party processors have to be PCI compliant?**
- **A:** Yes. Merely using a third-party company does not exclude a company from PCI compliance. It may cut down on their risk exposure and consequently reduce the effort to validate compliance. However, it does not mean they can ignore PCI.

- **Q: What are the penalties for noncompliance? A:** The payment brands may, at their discretion, fine an acquiring bank $5,000 to $100,000 per month for PCI compliance violations. The banks will most likely pass this fine on downstream till it eventually hits the merchant.

CUNA
TECHNOLOGY COUNCIL

Documentation

- Policies, procedures and documentation are a huge component of the standard.

TRUST-CC™
Devoted to Banking, Tecnically Superior, Trusted℠

CUNA TECHNOLOGY COUNCIL

Primary Account Number

- ***The primary account number (PAN) is the defining factor for cardholder data*.** If cardholder name, service code, and/or expiration date are stored, processed, or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected in accordance with all applicable PCI DSS requirements.
- First Six, **Middle Six**, Last Four

TRUST-CC™

Devoted to Banking, Tecnically Superior, Trusted™

CUNA TECHNOLOGY COUNCIL

Some PAN Details…

		Data Element	Storage Permitted	Render Stored Data Unreadable per PA-DSS Requirement 2.3
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[1]	Full Track Data [2]	No	Cannot store per PA-DSS Requirement 1.1
		CAV2/CVC2/CVV2/CID[3]	No	Cannot store per PA-DSS Requirement 1.1
		PIN/PIN Block[4]	No	Cannot store per PA-DSS Requirement 1.1

PA-DSS Requirements 2.2 and 2.3 apply only to PAN. If PAN is stored with other elements of cardholder data, only the PAN must be rendered unreadable according to PA-DSS Requirement 2.3.

Sensitive authentication data must not be stored after authorization, even if encrypted. This applies even where there is no PAN in the environment.

TRUSTCC

Devoted to Banking, Tecnically Superior, Trusted℠

Card Data Environment

- Those systems and networks that process, store or transmit cardholder data.

- **Q: What if a merchant refuses to cooperate? A:** PCI is not, in itself, a law. The standard was created by the major card brands such as Visa, MasterCard, Discover, AMEX, and JCB. At their acquirers/service providers discretion, merchants that do not comply with PCI DSS may be subject to fines, card replacement costs, costly forensic audits, exclusion, etc., should a breach event occur.

CUNA
TECHNOLOGY COUNCIL

TRUST-CC™

Devoted to Banking, Tecnically Superior, Trusted℠

Merchants (Merchant Banks)

http://usa.visa.com/merchants/protect-your-business/cisp/merchant-pci-dss-compliance.jsp#anchor_4

- Merchant banks are responsible for ensuring that all of their merchants comply with the PCI Data Security Standard (DSS) requirements; however, merchant compliance validation has been prioritized based on the volume of transactions, the potential risk, and exposure introduced into the payment system.

EMV Impact

- TIP rewards merchants that have invested in EMV technology by eliminating the requirement to validate compliance with the Payment Card Industry Data Security Standard (PCI DSS) for any year in which at least 75 percent of the eligible merchant's Visa transactions originate from dual-interface EMV chip-enabled terminals.

CUNA TECHNOLOGY COUNCIL

Merchant Levels

- All merchants will fall into one of the four merchant levels based on Visa transaction volume over a 12-month period. Transaction volume is based on the aggregate number of Visa transactions (inclusive of credit, debit and prepaid) from a merchant.

TRUST-CC™

Devoted to Banking, Tecnically Superior, Trusted℠

Merchant Levels

- Any entity, including merchants, that stores, processes or transmits Visa cardholder data must be PCI DSS compliant. In addition to adhering to the PCI DSS, compliance validation is required for Level 1, Level 2, and Level 3 merchants, and may be required for Level 4 merchants.

CUNA
TECHNOLOGY COUNCIL

Level 1: Over 6M Visa Transactions

- Annual Report on Compliance (ROC) by a Qualified Security Assessor (QSA) or internal auditor.
- Quarterly network Scan by Approved Scan Vendor (ASV)
- Attestation of Compliance

TRUSTCC™
Devoted to Banking, Tecnically Superior, Trusted™

CUNA
TECHNOLOGY COUNCIL

Level 2: 1M to 6M Visa Transactions

- Annual Self Assessment Questionnaire (SAQ)
- Quarterly network Scan by Approved Scan Vendor (ASV)
- Attestation of Compliance

TRUSTCC™
Devoted to Banking, Tecnically Superior, Trusted℠

CUNA
TECHNOLOGY COUNCIL

Level 3: 20k to 1M Visa Transactions

- Annual Self Assessment Questionnaire (SAQ)
- Quarterly network Scan by Approved Scan Vendor (ASV)
- Attestation of Compliance

TRUSTCC™
Devoted to Banking, Tecnically Superior, Trusted℠

CUNA TECHNOLOGY COUNCIL

Level 4: Less than20k Visa Transactions

- Annual Self Assessment Questionnaire (SAQ) Recommended
- Quarterly network Scan by Approved Scan Vendor (ASV)
- Compliance Validation as Set by Bank

TRUSTCC™

Devoted to Banking, Tecnically Superior, Trusted℠

CUNA
TECHNOLOGY COUNCIL

TRUST-CC™

Devoted to Banking, Tecnically Superior, Trusted℠

CUNA TECHNOLOGY COUNCIL

Compliance Confirmation for Banks and Credit Unions

VISA

Visa PCI DSS Data Security Compliance Program

Overview

The **Payment Card Industry Data Security Standard (PCI DSS)** is a comprehensive set of international security requirements for protecting cardholder data. The PCI DSS was developed by Visa and the founding payment brands of the PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures on a global basis.

These 12 requirements are the foundation of Visa's data security compliance program known as the *Account Information Security (AIS) Program*. This program was formerly known as the *Cardholder Information Security Program (CISP)* in the U.S.

Payment Card Industry Data Security Standard (PCI DSS)

- **Build and Maintain a Secure Network**
  1. Install and maintain a firewall configuration to protect data
  2. Do not use vendor-supplied defaults for system passwords and other security parameters
- **Protect Cardholder Data**
  3. Protect stored cardholder data
  4. Encrypt transmission of cardholder data and sensitive information 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 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

Every piece of cardholder account information that passes through the Visa payment system is vital to our business. Without proper safeguards in place, this information can be vulnerable to internal and external compromise, leading to fraud and loss of consumer confidence. The goal of Visa's security programs is to ensure the highest standard of due diligence to protect sensitive cardholder data from hackers and fraudsters.

About the Program

What is PCI DSS?

The PCI DSS protects Visa cardholder data wherever it resides.

Who Needs to Comply?

All Visa acquirers and issuers must comply, and must also ensure the compliance of their merchants and service providers who store, process, or transmit Visa account numbers. This program applies to all payment channels including card present, mail/telephone order, and e-commerce.

How Does it Work?

To achieve PCI DSS compliance, all Visa acquirers, issuers, merchants and service providers must adhere to the PCI DSS requirements set forth by the PCI Security Standards Council, which offers a single approach to safeguarding sensitive data for all card brands. Businesses may also be required to validate PCI DSS compliance in accordance with payment card brand requirements.

Why is it Important?

By complying with the PCI DSS, entities can protect their business and their customers while building a culture of security that benefits all parties in the payment system.

What To Do If Compromised

In the event of a security incident, Visa acquirers, issuers, merchants, and service providers must take immediate action to investigate the incident, limit the exposure of cardholder data, notify Visa, and report investigation findings. Visa's What To Do If Compromised guide, which can be found online at www.visa.com/cisp, contains step-by-step guidelines to assist clients, merchants, and service providers through a security incident.

For More Information

A detailed description of Visa's payment system security compliance programs including PCI DSS compliance and validation requirements, payment application security mandates, and PIN security and key management requirements can be found at www.visa.com/CISP. In addition, Visa publishes data security alerts, bulletins and webinar presentations; all are available for download.

TRUSTCC™

Devoted to Banking, Tecnically Superior, Trusted™

CUNA
TECHNOLOGY COUNCIL

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	**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 cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	**5.** Protect all systems against malware and regularly update anti-virus software or programs **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.** Identify and authenticate access to system components **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 for all personnel

TRUSTCC™
Devoted to Banking, Tecnically Superior, Trusted℠

CUNA
TECHNOLOGY COUNCIL

Specific Requirements

PCI Security Standards Council

Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures

Version 3.0
November 2013

TRUSTCC™
Devoted to Banking, Tecnically Superior, Trusted℠

CUNA
TECHNOLOGY COUNCIL

TRUST-CC™

Devoted to Banking, Tecnically Superior, Trusted℠

CUNA
TECHNOLOGY COUNCIL

Action Plan

- Understand DSS/PIN and know your responsibilities
- Read the requirements and testing procedures
- Ensure policies and processes are compliant
- Ensure vendors and merchants are compliant

TRUST-CC™
Devoted to Banking, Tecnically Superior, Trusted℠

CUNA
TECHNOLOGY COUNCIL

Keys to Success

- Shrink the Card Data Environment
- Make compliance routine
- Monitor closely
- Test whether required or not
- Get help where needed

TRUSTCC™
Devoted to Banking, Tecnically Superior, Trusted℠

CUNA
TECHNOLOGY COUNCIL

Wrap Up

TRUST-CC™
Devoted to Banking, Tecnically Superior, Trusted℠