

THE AUDITOR'S REPORT

NEWSLETTER

A Publication of Nearman, Maynard, Vallez, CPAs & Consultants, P.A.

COMPLIANCE CORNER II

What is PCI and do you have to be PCI compliant?

PCI stands for Payment Card Industry, and it consists of the 5 major credit card brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. The Payment Card Industry has established specific requirements for organizations to help protect customer account data, and through their joint efforts, the PCI Data Security Standard was created in order to enhance payment account data security by requiring the adoption of consistent data security measures on a global basis. Since September 7, 2006, the PCI Security Standards Council (PCI SSC) owns, maintains, and distributes the PCI Data Security Standard (DSS).

The PCI DSS is a security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. There are six categories of the PCI DSS with twelve requirements as per the VISA website:

(http://usa.visa.com/merchants/risk_management/cisp_overview.html).

You can also download the PCI DSS at www.securitystandards.org/pdfs/navigating_pci_dss_v1-1.pdf. They are as follows:

Build and maintain a secure network:

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. Use and regularly update anti-virus software
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. 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

According to the VISA Cardholder Information Security Program (CISP) Group and the MasterCard Site Data Protection (SDP) Program, anyone who is storing, processing or transmitting cardholder data must be PCI DSS compliant; specifically if the primary account number (PAN) is stored, processed, or transmitted.

Each card issuer has its own criteria for assigning merchant and validation compliance levels, with VISA and Mastercard being the most stringent. Generally, there are four levels of PCI DSS compliance, based on the number of annual transactions and whether you are considered a merchant or a service provider as defined by the payment brand. These levels determine whether you are required to have an on-site data security audit or can complete a self-assessment questionnaire. All levels are required to conduct quarterly network scans as part of their PCI DSS compliance program.

For those organizations that can complete the self-assessment questionnaires and in order to help merchants and service providers evaluate their compliance with PCI DSS, the PCI Security Standards Council developed and published Self-Assessment Questionnaires (SAQ).

There are five SAQ validation categories; the first four are based on how merchants are storing, processing, or transmitting cardholder data and the fifth category applies to all merchants who do not fit into the first four categories and all service providers defined by a payment brand as eligible to complete an SAQ. (For more information on the SAQs, see the PCI Security Standards Council's website at https://www.pcisecuritystandards.org/pdfs/instructions_guidelines_v1-1.pdf.)

In October 2008, the PCI Security Standards Council will release version 1.2 of the PCI DSS. The updated version will not introduce any new core requirements beyond the 12 mentioned above; its purpose is to clarify existing technical requirements, eliminate overlapping sub-requirements, and provide further clarification on scoping and reporting requirements.

A security breach and subsequent compromise of cardholder data has far-reaching consequences to include regulatory notification requirements (under NCUA Regulation 748), loss of reputation, loss of members, potential financial liabilities, and legal implications. Complying with PCI DSS is also a contractual requirement, and each payment brand can levy fines for non-compliance with its PCI DSS compliance program. For more information and to determine if your credit union must be PCI compliant, contact your payment brand's risk management division or visit the PCI Security Standards Council's website at www.pcisecuritystandards.org.

*Jennifer Hoskins, CPA, MPA, CTGA
Partner*