

---

## The PCI Data Security Standard:

It's Everywhere Your Credit Card Data Wants to Be

---

- page 2** Introduction
- page 2** The Basics of the PCI DSS: Who Must Comply, Compliance Requirements, Validation Requirements and Sanctions
- page 4** Compliance Requirements: 12 Steps to Data Security
- page 5** Validation Requirements: Maintaining and Demonstrating Compliance
- page 6** Arriving Where *You* Want to Be: PCI Implementation

## Introduction

A major advertising campaign by Visa states that the card is accepted “everywhere you want to be.” Unfortunately (and through no fault of Visa), a great deal of credit card data and other sensitive information has ended up in a lot of places that people would rather want it *not* to be. It seems that not a day goes by without reports of a high-profile credit card or credit data loss or compromise. The Washington Post has dubbed 2005 “the year of the data breach<sup>2</sup>.”

Unfortunately, these events are usually followed by calls in the press and government for additional data protection legislation. Representative Edward Markey of Massachusetts advertising cited the infamous CardSystems, Inc. security breach (causing the theft of up to 40 million credit card records) as an event that “only underscores the need for new federal legislation to protect American consumers<sup>3</sup>.” The rash of data loss and compromise incidents even caused the CISO of one of the victimized companies to remark that “Intervention is good... but the toughest part about legislation right now is you don't know where it's coming from and you don't know what to expect<sup>4</sup>.”

Long before these recent incidents and calls for legislation, however, Visa created a private standard known as CISP, or the Cardholder Information Security Program, which applied to all Merchants and Service Providers that handle Visa payments or card data. This program began in 2001, but more recently, Visa and American Express, Diner's Club, Discover, JCB and MasterCard collaborated to create a new set of standards, based on CISP, known as the PCI (DSS) (Payment Card Industry Data Security Standard.) All merchants and service providers that handle, transmit, store or process information concerning any of these cards, or related card data, were required to be compliant with PCI as of June 30, 2005.

In September 2006, the PCI Security Standards Council released the new PCI Data Security Standard v1.1. This paper discusses the basic requirements of PCI, with a focus on the administrative and technical elements of the program. It also reviews the validation requirements of the standard and potential sanctions for failure to comply.

## The Basics of PCI:

### Who Must Comply, Compliance Requirements, Validation Requirements and Sanctions

Before exploring the details of the compliance and validation requirements, it is important to have a basic working knowledge of the “who, what, why and when” of PCI. First, it is important to note that PCI is not a law: It is a private security standard that members, merchants and service providers must follow pursuant to their contracts with the credit card companies. Although PCI is not a law, it is enforceable by the credit card companies through contractual penalties or sanctions that include revocation of the company's right to accept or process credit card transactions.

PCI applies to all members, merchants and service providers that store, process or transmit cardholder data<sup>5</sup>, whether that data is received in a point of sale, phone, e-commerce or other type of transaction. It applies

---

<sup>1</sup> Daniel J. Langin is the principal of Daniel J. Langin, Attorney at Law, LLC. He has over 16 years of experience in private and corporate practice, including ten years of experience in technology, insurance coverage and intellectual property litigation and counseling. For more information, see [www.langinlaw.com](http://www.langinlaw.com) or contact Daniel at (913) 661-2430 or [dlangin@langinlaw.com](mailto:dlangin@langinlaw.com). This article is provided for general educational and informational purposes. It is not intended to provide legal advice.

<sup>2</sup> “Firm Says Up to 40m Credit Card Files Stolen; MasterCard Points to Computer Virus,” Boston Globe June 18, 2005.

<sup>3</sup> Id.

<sup>4</sup> “Sidebar: Users Want Pragmatic Security Rules,” Computerworld June 27, 2005 (quoting Rich Baich, CISO of ChoicePoint, Inc.).

<sup>5</sup> See Visa USA, Inc. Payment Card Industry Data Security Standard, Version 1.1 (September, 2006) (available at [www.usa.visa.com](http://www.usa.visa.com)).

to all “system components,” which PCI defines as “any network component, server, or application included in, or connected to, the cardholder data environment<sup>6</sup>.” Although the details differ slightly for each of the credit card companies that require PCI compliance, the PCI DSS is made up of a set of 12 individual compliance requirements (each of which includes more detailed compliance steps), organized around six primary goals, all of which add up to a comprehensive information security program for protecting credit card numbers and other sensitive cardholder data from loss or compromise.

In addition to the compliance requirements, PCI also contains ongoing validation requirements. These requirements differ somewhat from one credit card company to another, but the most comprehensive requirements (Visa and MasterCard) include three levels of validation: (1) an on-site security audit; (2) a self-assessment questionnaire, and; (3) a network scan. The level of validation required, and the frequency of validation efforts, depends upon the rating assigned to the Merchant or Service Provider under PCI, which is based on risk and transaction or account volume.

Last, the PCI program also includes monetary penalties and other contractual sanctions for failure to meet its requirements. For example, under the Visa PCI program, members can be fined up to \$500,000 per incident if any merchant or service provider that is not PCI-compliant is compromised. Visa members who fail to immediately notify Visa of a suspected or known loss or theft of transaction information may be fined \$100,000 per incident, plus additional fines if a PCI violation presents immediate and substantial risks to Visa and its members.

Failure to meet PCI can also result in suspension or revocation of a company’s right to accept or process credit card transactions. Of course, loss of reputation and potential business is also a motivation to comply, as noted by Chris Noel of Solutionary, Inc.:

I wouldn’t want to be a merchant issuing a press release saying, ‘I’m sorry, your data is compromised and here’s an 800 number for you to report any fraudulent transactions.’ It can’t help for you to be in a position where you’ve not protected the most precious asset your customers entrusted you with—their financial information<sup>7</sup>.

With these basics in mind, a detailed review of the 12 compliance requirements of PCI is necessary to start the path to compliance.

---

<sup>6</sup>Id.

<sup>7</sup>“Keep It Safe; Retailers are coming around to the card companies’ security programs,”Internet Retailer (May 2005)

### Compliance Requirements: 12 Steps to Data Security

As noted above, the PCI compliance requirements consist of 12 major requirements organized into six primary categories. Although a number of the laws concerning IT security (such as the Gramm-Leach-Bliley Act and HIPAA) are organized into administrative, technical and physical requirements, PCI was not organized along these lines by its authors. For those interested in comparing PCI to the requirements of such security laws, however, this paper breaks the 12 PCI requirements down into their administrative, physical and technical elements in the table below. Because the PCI DSS contains numerous detailed sub-requirements, this table uses sample elements to illustrate each requirement rather than containing a comprehensive list of all elements. The PCI DSS consists of 12 basic requirements and corresponding sub-requirements categorized as follows:

| PCI DSS                                     |  |
|---|--|
| Build and Maintain a Secure Network         | <ol style="list-style-type: none"> <li>1. Install and maintain a firewall configuration to protect data</li> <li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ol>            |
| Protect Cardholder Data                     | <ol style="list-style-type: none"> <li>3. Protect stored data</li> <li>4. Encrypt transmission of cardholder data and sensitive information across public networks</li> </ol>  |
| Maintain a Vulnerability Management Program | <ol style="list-style-type: none"> <li>5. Use and regularly update anti-virus software</li> <li>6. Develop and maintain secure systems and applications</li> </ol>   |
| Implement Strong Access Control Measures    | <ol style="list-style-type: none"> <li>7. Restrict access to data by business need-to-know</li> <li>8. Assign a unique ID to each person with computer access</li> <li>9. Restrict physical access to cardholder data</li> </ol> |
| Regularly Monitor and Test Networks         | <ol style="list-style-type: none"> <li>10. Track and monitor all access to network resources and cardholder data</li> <li>11. Regularly test security systems and processes</li> </ol>   |
| Maintain an Information Security Policy     | <ol style="list-style-type: none"> <li>12. Maintain a policy that addresses information security</li> </ol>  |

**Validation Requirements: Maintaining and Demonstrating Compliance**

As noted above, implementing the compliance requirements is only the start of the process. PCI contains a set of validation requirements that are required to ensure that companies continue to meet the PCI standard on an ongoing basis. The validation steps for the PCI DSS are described in the table below:

| Level | Validation Action  | Validated By  | Due Date  |
|-------|--|---|---|
| 1     | Annual On-site PCI Data Security Assessment and Quarterly Network Scan | Qualified Security Assessor or Internal Audit if signed by Officer of the company<br>Approved Scanning Vendor | 9/30/04<br><br>New level 1 merchants have up to one year from identification to validate. |
| 2     | Annual PCI Self-Assessment Questionnaire and Quarterly Network Scan    | Merchant<br>Approved Scanning Vendor  | New level 2 merchants: 9/30/2007  |
| 3     | Annual PCI Self-Assessment Questionnaire and Quarterly Network Scan    | Merchant<br>Approved Scanning Vendor  | 6/30/05   |
| 4     | Annual PCI Self-Assessment Questionnaire and Quarterly Network Scan    | Merchant<br>Approved Scanning Vendor  | Validation requirements and dates are determined by the merchant's acquirer               |

Levels are based on volume and/or risk, i.e.:

| Level                    | Description  |
|--------------------------|--|
| Merchant Level 1         | Any merchant-regardless of acceptance channel-processing over 6,000,000 Visa transactions per year.<br>Any merchant that has suffered a hack or an attack that resulted in an account data compromise.<br>Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.<br>Any merchant identified by any other payment card brand as Level 1. |
| Merchant Level 2         | Any merchant-regardless of acceptance channel-processing 1,000,000 to 6,000,000 Visa transactions per year.  |
| Merchant Level 3         | Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year.   |
| Merchant Level 4         | Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants-regardless of acceptance channel-processing up to 1,000,000 Visa transactions per year.   |
| Service Provider Level 1 | All VisaNet processors (member and Nonmember) and all payment gateways.  |
| Service Provider Level 2 | Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 Visa accounts/ transactions annually.  |
| Service Provider Level 3 | Any service provider that is not in Level 1 and stores, processes, or transmits fewer than 1,000,000 Visa accounts/ transactions annually.   |

## Arriving Where You Want to Be: PCI Implementation

The previous tables make it clear that most of the challenge in implementing PCI lies in the technical and administrative aspects of the standard. This is not surprising, given that most of the risk to credit card data arises from exploits that target technical and administrative weaknesses in security. The fact that PCI requires ongoing validation of security efforts, coupled with the fact that security exploits are constantly changing, make it clear that companies subject to PCI cannot implement “install and forget” solutions. John Shaughnessy, senior vice president of fraud management for Visa USA, has remarked that PCI is “raising the security bar,” and that compliance is “going to be an ongoing process<sup>8</sup>”

Even the best security efforts will fail, however, if they are not coordinated with overall business processes to ensure that persons or departments within the company are not changing security safeguards or skirting policies and procedures. For example, after the revelation that a hacker may have compromised up to 40 million MasterCard credit card accounts, CardSystems, Inc. (the processor of those credit cards) admitted that 200,000 of the affected records had been kept in a separate database used for research purposes, in violation of policy.

Furthermore, companies need to be prepared to back up validation efforts with records that demonstrate compliance and will back up an audit of compliance measures. PCI contains numerous requirements for logging, tracking and the ability to present auditable records. PCI also requires the implementation of measures that will detect whether, how and when unauthorized changes are made to systems or records. Section 10.5.5 of PCI requires the use of “file integrity monitoring/change detection software on logs to ensure that existing log data cannot be changed without generating alerts.” In other words, when the third party, independent assessors who have been certified by the credit card companies drop by to perform the annual on-site audit, companies must be prepared to produce clear, comprehensive and reliable records demonstrating compliance.

Nigel Tranter, a partner at a company which conducts security audits for payment processors, predicts “we will see fines being levied and some fairly strong-arm tactics applied<sup>9</sup>.” To respond to the challenges of PCI, companies should combine technical measures, administrative best practices and sound IT decision making into a program of change auditing. By making sure that PCI DSS requirements are in place, that reliable records exist to support compliance during validation and that the company can track and demonstrate any changes, the companies subject to PCI can be “where they want to be” when audit time rolls around.

---

<sup>8</sup> “Retailers Facing Critical IT Security Deadline,” CIO Insight April 26, 2005.

<sup>9</sup> “Banks Scramble To Contain Damage From CardSystems Hacking Incident,” Bank Systems and Technology (June 22, 2005).

---



Audit Change. Prove Control.

[www.tripwire.com](http://www.tripwire.com)

US TOLL FREE: 1.800.TRIPWIRE MAIN: 503.276.7500 FAX: 503.223.0182  
326 SW Broadway, 3rd Floor Portland, OR 97205 USA

[www.tripwire.com/intl/uk](http://www.tripwire.com/intl/uk)

TRIPWIRE UK: +44 207 618 6512 FAX: +44 207 618 8001  
78 Cannon Street London EC4N 6NQ UK