



# Continuous PCI Compliance

A Crucial Initiative for Any Retailer

by **Anna McCullough** CPA, CFE, and CFF



# Continuous PCI Compliance: A Crucial Initiative for Any Retailer

Written by Anna McCullough, CPA , CFE, CFF  
*December 5, 2009*

## Introduction

The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC). The standard was created in 2004 to help organizations that process card payments prevent credit card fraud through increased controls around data and its exposure to compromise. The standard applies to all organizations which hold, process, or pass cardholder information from any card branded with the logo of one of the card brands.

As of August 2009, the PCI SSC announced the move from version 1.2 to version 1.2.1 for the purpose of making minor corrections designed to create more clarity and consistency among the standards and supporting documents, which is currently in effect. The Federal Reserve, the Office of Thrift Supervision and the National Credit Union Administration announced the enactment of comprehensive new rules regarding card practices. These rules will take effect on July 1, 2010 in conjunction with the PCI SSC enacting v. 2.0. It is a fast changing compliance environment, causing headaches and concern for merchants of all levels.

Although it seems that PCI Compliance is just part of being in the retail business, it is truly important. Serious cost and loss can occur when an organization is not in compliance. For example, hundreds of credit and debit card holders appear to have been victims of a nationwide data theft carried out against Heartland Payment Systems, which processes cards for 250,000 restaurants, retailers and other businesses.

As a result of the Heartland data breach, several Maine credit unions have been told by Visa and MasterCard that fraudulent charges were placed on members' cards between May 16 and August 19, 2008, according to Jon Paradise, a spokesman for the Maine Credit Union League. Many of the charges were tallied at Wal-Mart stores in Texas, he said. According to the Washington Post (Brian Krebs), tens of millions of people may be affected. A spokesman for Heartland indicated they do not know how long the malicious software was in place, how it got there or how many accounts may have been compromised. The stolen data includes names, credit and debit card numbers and expiration dates. As of the end of May 2009, more than 656 institutions have been impacted. And, as of October the number of records seems to have stabilized at 130 million.

Although we often hear of the retail giants being victims of data theft, it is not just the large retailers who need to be concerned. In fact, an article in the Wall Street Journal titled, "In Data Leaks, Culprits Often Are Mom, Pop Credit-Card Industry Tries to Add Safeguards; Honest Errors Common" emphasize the fact that every business, no matter how small, must be aware. Further, Jennifer Fischer, SVP – Payment Security System Compliance for Visa, stated, "Visa continues to see small merchants most frequently targeted by hackers."

PCI Compliance is a concern to all organizations, no matter how large or small. Because everyone must comply with PCI regulations, the next question becomes one of cost.

## What are the PCI DSS Standards?

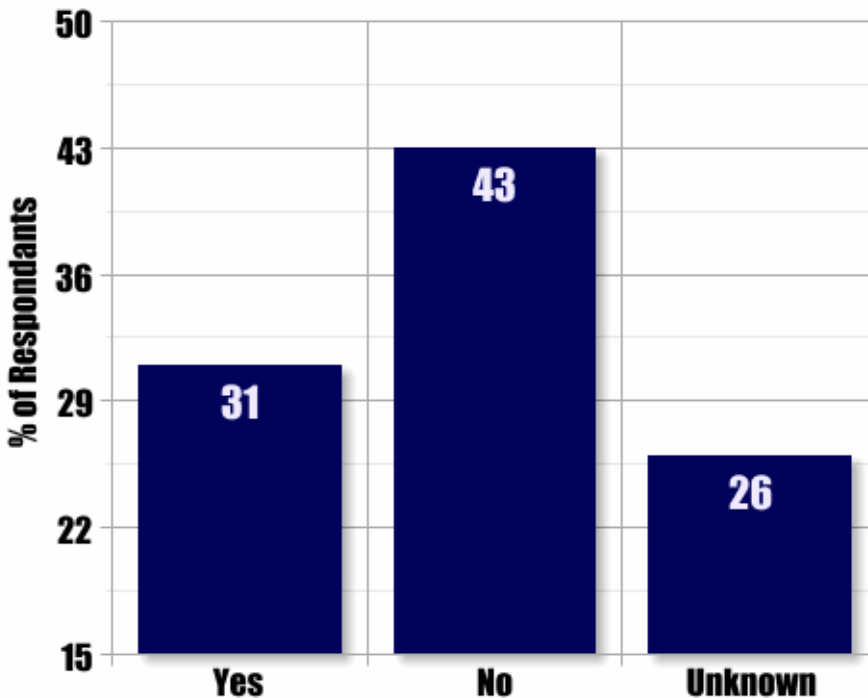
The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

There are 6 control objectives resulting in 12 requirements that organizations must meet, as follows:

1. *Build and Maintain a Secure Network*  
*Requirement 1:* Install and maintain a firewall configuration to protect cardholder data  
*Requirement 2:* Do not use vendor-supplied defaults for system passwords and other security parameters
  
2. *Protect Cardholder Data*  
*Requirement 3:* Protect stored cardholder data  
*Requirement 4:* Encrypt transmission of cardholder data across open, public networks
  
3. *Maintain a Vulnerability Management Program*  
*Requirement 5:* Use and regularly update anti-virus software  
*Requirement 6:* Develop and maintain secure systems and applications
  
4. *Implement Strong Access Control Measures*  
*Requirement 7:* Restrict access to cardholder data by business need-to-know  
*Requirement 8:* Assign a unique ID to each person with computer access  
*Requirement 9:* Restrict physical access to cardholder data
  
5. *Regularly Monitor and Test Networks*  
*Requirement 10:* Track and monitor all access to network resources and cardholder data  
*Requirement 11:* Regularly test security systems and processes
  
6. *Maintain an Information Security Policy*  
*Requirement 12:* Maintain a policy that addresses information security

While the standard is meant to have a positive impact on merchants, consumers and the retail industry, many retailers are still questioning its effectiveness and necessity in light of the high-cost to comply. A recent poll of 201 IT and PCI compliance professionals reinforces this point. The study found that 57% of respondents either experienced a compliance control deficiency in the past year or did not know if they had a PCI compliance deficiency in the IT environment.

### Companies with Compliance Related Control Deficiencies (in the past year)



**SOURCE: Solidcore & Emagined Security PCI Survey (n=201)**

*Another recent poll conducted by Solidcore Systems and Emagined Security surveyed a group of 173 IT professionals responsible for PCI compliance, and found that only 6% were completely confident they would not experience a data breach following a successful PCI compliance assessment.*

### Is PCI DSS Compliance important to all sizes of merchants?

The cost and effort required by organizations to become PCI compliant depends upon the number of transactions of the organization. All merchants will fall into one of four levels. Level four merchants are defined as 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 million card transactions per year.

*According to Visa, Level 4 merchants handle fewer transactions than Levels 1, 2 and 3, but they account for more than 99 percent of the merchants that accept Visa.*

This segment of the market is an ultimate target for hackers and usually, Level 4 merchants do not have the technical expertise or the IT Staff, to properly secure card holder data. For all data breaches there are two primary risks: The internal risk of an employee obtaining a file that they shouldn't have, and an

external risk in a hacker. Unfortunately, the latter are becoming much more organized, better equipped, and specialize in cyber theft and fencing of this highly valuable cardholder data (includes numbers, expiration dates, and personally-identifiable information (PII)).

If an organization is assessed penalties due to non-compliance, 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 until it eventually hits the merchant. Furthermore, the bank will also most likely either terminate the relationship or increase transaction fees. Penalties are not openly discussed nor widely publicized, but they can be catastrophic to a small business. It is important to be familiar with the merchant account agreement, which should outline an organization's exposure.

## What is involved in becoming PCI Compliant?

There are three categories of cost associated with PCI Compliance:

### *Upgrading Infrastructure*

New components that might have to be installed to upgrade payment systems and security infrastructure include additional firewalls, upgraded anti-virus and anti-spyware software, secure wireless systems, data encryption technologies and file-integrity monitoring software.

### *Verifying Compliance (Assessment)*

In any corporate environment, it is critical to periodically assess the complete infrastructure, research, and analyze any potential weaknesses, and to develop remediation plans. With the heightened level of sophistication of attacks and increases in the number of hackers, having a strong network security strategy is imperative. Security in any environment is an evolving process, the purpose of which is to ensure the continuity of the network and the systems connected to it. IT Security Assessments should be an integral part of any enterprise risk and security process.

### *Sustaining Compliance*

Just because an organization is compliant today, does that mean it will be compliant tomorrow? Unfortunately the answer to that question is "no," which means that ongoing compliance efforts must be incorporated by organizations. Essentially, PCI is a good starting point and a good standard to audit against, but just "hitting the checklist" isn't going to create good security. Although PCI is a point-in-time audit, maintaining compliance is not. In order to sustain compliance, organizations have to go beyond the checklist.

## There are three categories of cost associated with PCI Compliance – which one causes the most concern?

The key issue that is overlooked by an enterprise, whether Level 1, 2, 3, or 4, is the need to sustain compliance. An organization can be considered "PCI Compliant" at any moment in time. However, there must be initiatives to ensure that the state of compliance is maintained on an ongoing basis.

As an example, suppose a level 4 merchant completes self assessment questionnaire (SAQ) as required. The merchant then completes and obtains evidence of a passing vulnerability scan with a PCI SSC Approved Scanning Vendor (ASV), where required.

***Note:** Network scanning does not apply to all merchants. It is required for Validation Type 4 and 5 – those merchants with external facing IP addresses. If cardholder data is electronically stored, or if processing systems have any internet connectivity, a quarterly scan by an approved scanning vendor is required.*

Suppose further that the very day after the merchant obtains evidence of a passing vulnerability scan, the merchant opens a new location. The PCI regulations state that if business locations process under the same Tax ID, then typically the requirement is only to validate once annually for all locations and submit quarterly passing network scans by an PCI SSC Approved Scanning Vendor (ASV).

Therefore, there is an immediate and true risk for the merchant who opened a new location that is not in compliance with that new location. In fact, the risk of potential non-compliance may go undetected until the next required validation (which occurs only annually) and/or the quarterly passing network scans.

The purpose of this illustration is to demonstrate that a merchant may be in compliance at a specific moment in time, but (as in this example), they immediately expose themselves to risk of non-compliance with a typical business activity such as opening a new location.

While this is one very simple example, the point remains clear that it is crucial for a retail organization to not only obtain, but to sustain, PCI compliance. Industry experts agree that merchants need more help than they believe they need, and by using a tool such as SecureAware®, an organization can create ongoing, sustained PCI compliance.

## Conclusion

### Continuous PCI Compliance with IT GRC

As the breaches at Heartland Payment Processing Systems and Hannaford Brothers have demonstrated, compliance with Payment Card Industry Data Security Standard (PCI DSS) does not guarantee bulletproof security. Favorable performance in an annual On-Site PCI Data Security Assessment or Self-Assessment Questionnaire (SAQ) is simply a snapshot of a company's status at one point in time and not proof of ongoing compliance. For example, Hannaford Bros received its PCI DSS compliance certification one day after it had been made aware of a two-month long breach of its network. The PCI Security Standards Council says that "compliance efforts must be a continuous process of assessment and remediation to ensure safety of cardholder data." Given this advice, as well as the examples of post-compliance breaches, the global retail community and its service suppliers have been propelled into a new era for PCI DSS compliance management. Not only must the retailer, bank or payment processor achieve compliance at a fixed point in time, it must also implement specific programs to manage and maintain compliance on an on-going basis. The concept of "Continuous Compliance" helps these market constituents save money on SAQs and audit / certification fees by Qualifies Security Assessors (QSAs). Ideally, a retailer should know its PCI DSS compliance status on a daily basis. While this may sound cost and resource prohibitive, the use of automated tools for IT Governance, Risk and Compliance (IT GRC) can provide the type of information and the security framework to make this a reality.

The clock is ticking on the July 1, 2010 deadline for complying with the Payment Card Industry Data Security Standards. Introduced in 2004, the standards were developed by the major credit-card companies as a guideline to help organizations that process card payments prevent credit-card fraud, hacking, and other security threats.

*It should be noted that the July 1, 2010 deadline applies to all levels – Level 1, 2, 3, and 4. It is imperative that a merchant become compliant by this date.*

Consumers are becoming increasingly aware of the dangers of identity theft due to compromised data and stolen credit card information. PCI compliance assures to customers that merchants are looking out for their safety and well-being. Approach it with that in mind, and compliance is transformed into a competitive edge and asset instead of a dreaded "must do."

While validating compliance with the PCI standard is a requirement, it is also an opportunity. Finding and fixing compliance gaps keeps an organization running smoothly and reputations intact.

The most crucial issue for an enterprise to understand is that compliance, at one moment in time, does not mean the same thing as a continuous, ongoing compliance program. Tools, such as SecureAware® from Lightwave Security, give an enterprise the confidence and competitive advantage that they are PCI compliant on an ongoing basis.

**Author:** Anna McCullough, CPA, CFE, CFF  
Strategist - PCI Initiatives  
[amccullough@lightwvsecurity.com](mailto:amccullough@lightwvsecurity.com)  
Lightwave Security  
1200 Abernathy Road / Suite 1700  
Atlanta, GA 30328  
Main: 800.616.8597

#### Sources:

[http://www.idtheftcenter.org/artman2/publish/lib\\_survey/ITRC\\_2008\\_Breach\\_List.shtml#breaches](http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml#breaches)

[http://online.wsj.com/article/SB119042666704635941.html?mod=sphere\\_ts](http://online.wsj.com/article/SB119042666704635941.html?mod=sphere_ts))

*Solidcore and Emagined Security PCI Survey*