

# Brown Smith Wallace, LLC

## Successful Software Selection Whitepaper Series

### How to Adhere to Payment Card Industry Data Security Standards

By Ron Schmittling, CPA/CITP, QSA, CISA, CIA

To learn more about PCI Compliance Review:

<http://www.bswllc.com/pci-review>

To learn more about IT Security and Privacy:

<http://www.bswllc.com/it-security-and-privacy>

#### PCI Compliance Primer

As consumers rely more on debit and credit cards as opposed to cash, merchants are facing increased risk exposures if they don't have proper security measures in place. Cyberthieves troll for information on merchant networks, which has resulted in significant security breaches that have made headlines.

In 2004, a consortium of credit card companies, including Visa, MasterCard, Discover and American Express, banded together to set Payment Card Industry (PCI) Data Security Standards. These standards direct merchants that process, store or transmit credit card information to maintain a secure environment. And if your business accepts credit or debit cards, the standards apply to you.

Business owners have to comply with those security standards and implement safeguards to protect customer information. This article will discuss how your company can meet PCI standards and protect against security breaches.

#### What is PCI compliance, and who must comply?

The three keywords for PCI compliance are process, store and transmit. If your organization processes, stores or transmits credit card information, you must maintain a secure environment as laid out by the PCI standards. So, if customers or vendors use debit or credit cards to make purchases from your business, you must be compliant. This includes meeting 12 standards, which can be broken down into six key areas: building and maintaining a secure network; implementing safeguards to protect cardholder data; maintaining a vulnerability management program; applying strong access control measures; regularly monitoring and testing network security; and enforcing an information security policy.

Your policy will ultimately drive the compliance process, so the first step is to take a security inventory of your business to determine how compliant it is, what security measures are in place and what weak spots must be addressed. An outside adviser with experience in security and privacy can provide feedback on how to structure a plan. This framework will set the tone for your internal compliance strategy and help protect your business.

## **How to Adhere to Payment Card Industry Data Security Standards?**

June 16, 2010

Page 2 of 6

PCI security standards are not laws; they are a method of self-imposed regulation by the consortium of credit card companies. There are no federal mandates in place, but there is a move in that direction since some states have started to pass laws or require organizations to comply with PCI Data Security Standards. This trend is expected to continue in association with the Data Breach Notification Laws movement.

### **What are the consequences of failing to comply with the standards?**

At their discretion, payment brands such as Visa or MasterCard can fine acquiring banks \$5,000 to \$10,000 a month for PCI compliance violations. Banks are likely to pass these fees on to noncompliant merchants. Many banks have begun notifying noncompliant merchants of their need to comply or face fines.

You should review your merchant agreement and note any penalties and fees for noncompliance, which can include prohibiting merchants from processing credit card transactions, higher processing fees and other restrictions. Any fraud loss associated with a compromise in security may be borne by the merchant starting on the date of the security breach. Depending on the level of security negligence, the FTC could become involved and impose significant federal fines, up to \$250,000 and/or up to five years in prison.

Not knowing is not a viable excuse for noncompliance and could cost you and your organization. It is your responsibility to understand your merchant agreement and what the PCI standards mean to your organization.

### **What steps can a company take to become PCI compliant?**

Compliance responsibility depends on your merchant level, and there are four levels as defined by PCI Data Security Standards. Level 1 merchants are those that process more than 6 million transactions a year. It is important to note the annual transactions are measured in volume, not dollars. Level 2 includes merchants that process 1 to 6 million transactions per year. Level 3 covers merchants with 20,000 to 1 million eCommerce transactions per year. Level 4 includes any merchant with fewer than 20,000 eCommerce transactions per year, and all other merchants with fewer than 1 million transactions annually.

Companies in Levels 2, 3 and 4 follow the same compliance process that includes completion of an annual self-assessment questionnaire and having quarterly network scans performed by a PCI Approved Scanning Vendor (ASV). The results are submitted to the merchant's bank. Level 1 merchants follow similar procedures, but also are required to have an annual on-site review completed by a Qualified Security Assessor (QSA), a PCI-certified provider and have an annual network penetration test performed. The QSA will submit the merchant's Report on Compliance to its merchant bank. The PCI Council lists ASVs and QSAs at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

### **Where should an organization start on its PCI compliance initiative?**

The most important step is to set an internal policy of how you'll address PCI compliance and information security. Too many times, organizations rush into identifying a new product they think will fix PCI compliance or information security problems instead of organizing their efforts around the organization's overarching policies and processes.

## How to Adhere to Payment Card Industry Data Security Standards?

June 16, 2010

Page 3 of 6

Once that policy has been defined and implemented, an organization can begin to enforce it and truly drive its compliance initiatives. But compliance starts with your information security policy and security controls. Many organizations struggle with where to start, as PCI compliance can be a daunting and complex task. Reaching out to a QSA to kick-start your PCI compliance efforts is a great first step.

### What are the PCI DSS main areas?

The actual PCI Data Security Standards include 12 major requirements for validation and certification under six main auditing areas or "control objectives". All of the compliance areas include basic security rules that most merchants and service providers should already have in place, or have a familiarity with them when audited.

The six main control objectives for PCI DSS compliance and validation are as follows:

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

### What is a QSA?

QSA stands for Qualified Security Assessor. It is a certification obtained by experienced security consultants that enable them to conduct the on-site data security assessments for PCI DSS Compliance. QSA's are required to recertify every year by attending training provided by the PCI Council and passing a rigorous exam. A recertifying QSA must also obtain annual professional education credits from training and other experiences in order to retain certification. May QSA's also maintain other certifications through their work as security practitioners such as CISSP, CISA, CISM, etc.

### What are the requirements for becoming a QSA?

The PCI Council requires all QSA's to be full time employees of a Validated QSA company. The security professional must complete a thorough application process with the PCI Council and undergo and pass its three-day QSA training course. A closed-book exam is administered which must also be passed to receive the official QSA certification.

In addition, the QSA must meet the following minimum requirements, submit a current resume with the PCI Council, and complete a background check from the QSA company:

- CISSP, CISA or CISM Certificate
- 5 Years of IT Security experience

## **How to Adhere to Payment Card Industry Data Security Standards?**

June 16, 2010

Page 4 of 6

### **Why are QSAs important?**

PCI QSAs are trained by the PCI Standards Council to understand the intent and rigor required to meet the PCI requirements. Only a QSA can certify PCI compliance and working with a QSA is the best way to ensure your implemented controls will meet the PCI compliance requirements. And of course, getting it right the first time saves time and money.

QSAs are required to strictly adhere to the DSS audit procedures document and complete the mandatory Report on Compliance required for PCI certification and validation on behalf of the merchant or service provider.

Many QSA's help companies perform their annual PCI self-assessments also. Self-assessments are much easier said than done, as most merchants and service providers simply lack the knowledge and understanding of PCI to self-assess with no help. A QSA can help bridge the knowledge gap and quickly assist with completing your self-assessment.

Further, a QSA can also assist in recommending various hardware and software solutions for PCI compliance along with giving a company excellent guidance on how to meet the rigorous demands of PCI Compliance. When it comes to compliance and certification for PCI, you need to use a QSA.

### **What types of services do QSA's typically provide?**

QSA's typically provide the following types of services:

- On-Site Data Security Assessments (PCI "Audits"),
- PCI Gap Analysis or Readiness Assessments,
- Remediation Services for areas of PCI deficiency,
- Project Management,
- General PCI consulting and advice.

Depending on the size of the company, its complexity, and the number of distinct credit card processes, most engagements will last anywhere from 1 - 6 months.

Level-1 Merchants and Level 1-2 Service Providers are required to have a QSA to conduct their annual on-site data security assessment. Level 1-2 qualifiers are that they have more than 6 million transactions. Level 2-4 Merchants and Level-3 Service Providers do not have required QSA audits and may use the PCI Self-Assessment Questionnaire to self-certify.

## **How to Adhere to Payment Card Industry Data Security Standards?**

June 16, 2010

Page 5 of 6

### **What are the pros and cons of hiring a QSA versus doing it yourself?**

There are pros and cons for both ways of performing PCI compliance, but the pros outweigh the cons in selecting a QSA to assist with your PCI compliance initiatives. QSAs provide third-party validation which proves 'due diligence', in addition, they know the data security standard and how it is to be applied to different types of organizations. The cons are the usually the cost of hiring a QSA. Yet, the costs to the organization when considering 'doing it yourself' should also be considered - that is, resources needed to assist with PCI compliance plus resources from other strategic, profit-generating initiatives. Another con to consider is that it can be difficult to get up to speed on all PCI requirements, which could provide an unfortunate opportunity for merchants to miss key areas, controls, and dates. In the long run, it may be far more economical to hire a QSA.

### **What are the benefits of using a QSA and becoming PCI compliant?**

In the past few years as cybercrime has sky-rocketed it's necessary to do more to protect companies and customers alike. The PCI requirements might seem difficult to get a grasp on; however, they are beneficial for customers, merchants, and the credit card industry. Merchant and service providers have to meet a number of measures from QSAs and ASVs in order to be PCI Compliant. There are a number of significant benefits to becoming PCI Compliant and utilizing a QSA to assist, including:

- 'Trust'. Consumers greatly benefit from doing business with PCI Compliant companies because it means all of their sensitive information is kept both safe and secure.
- Means that your business has been checked for security weaknesses by a qualified, information security professional.
- It provides an incredibly solid structure for greatly improving security, operation and audit performance by a having an independent assessment performed.
- It sets any business up to be more stable and to avoid infections or security disasters.
- Without it you can't process credit card information and a merchant cannot get by without processing credit cards nowadays.
- Merchants who are PCI compliant are offered some level of protection from the fines if you should happen to be breached. If you are compliant at the time you suffer an attack, you may have a 'safe harbor', along with connections to a QSA that can assist in shepherding the process to minimize the breach effect on both your customers and business.

## How to Adhere to Payment Card Industry Data Security Standards?

June 16, 2010

Page 6 of 6

### About The Author

#### **Ron Schmittling, CPA/CITP, QSA, CISA, CIA, Security and Privacy Practice Leader at Brown Smith Wallace, LLC**

Ron's 18+ years of experience include more than five years in senior-level technical leadership roles at a major financial services firm, as well as, positions in information security and technology consulting for several international organizations. Ron is a thought leader, frequent speaker and author on topics in the information security and PCI compliance arena. Ron is a member of the American Institute of Certified Public Accountants (AICPA), the Illinois CPA Society (ICPAS), the Missouri Society of CPAs (MSCPA), ISACA, Institute of Internal Auditors (IIA), InfraGard, International High Technology Crime Investigation Association (HTCIA), Information Systems Security Association (ISSA), and the Institute of Computer Forensic Professionals (ICFP).

Schmittling can be reached at 314-983-1398 or [schmittling@bswllc.com](mailto:schmittling@bswllc.com).

### About The Brown Smith Wallace Security and Privacy Practice

The Brown Smith Wallace Security and Privacy Practice is a market leader in helping businesses, government, financial institutions, retailers, educational institutions, and healthcare groups and other organizations define the true risks in their environment and deploy the right solutions and technologies to ensure the continued success of day-to-day operations and objectives. Our services include attack and penetration testing, internal vulnerability assessments, security risk assessments, security training, social engineering tests, PCI compliance reviews, PCI readiness assessments, PCI ASV vulnerability scanning, privacy risk assessments, computer forensics, and many others.

For More Information

Contact:

Sara Nelson  
314.983.1393  
[snelson@bswllc.com](mailto:snelson@bswllc.com)



1050 North Lindbergh Boulevard, St. Louis, Missouri • 63132 • 314.983.1200 • [www.bswllc.com](http://www.bswllc.com)