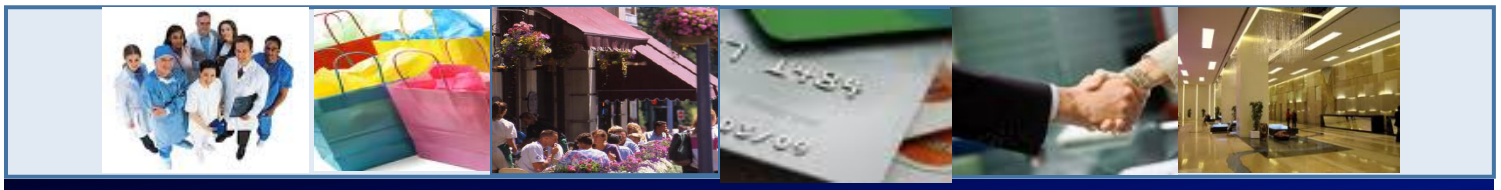

SUMMIT STRATEGIES

Summit Strategies Merchant Support:

# Understanding PCI DSS

## Understanding PCI DSS

**Protecting your cardholder information and reducing data theft.**

**The payment card industry is changing** — and with technological evolution comes the expansion of technology crimes. Data security breaches have become increasingly common, placing in harm's way the economic security of U.S. businesses and consumers. Every day, businesses just like yours encounter a very real threat from criminals intent on obtaining your customers' credit and debit card data.

**The Payment Card Industry Data Security Standard (PCI DSS)** was created by Visa®, MasterCard®, American Express® and Discover® Financial Services to protect cardholder information and reduce data theft. PCI DSS establishes security requirements for members, businesses and service providers. PCI DSS applies to all organizations involved in credit card processing. One of the most significant PCI DSS requirements is that you may not store magnetic-stripe data after an authorization is obtained on a credit card. Accordingly, magnetic-stripe data must be purged from your records, and from any system you use, after authorization.

**The PCI DSS protocols benefit businesses of all sizes in several ways:**

> Being PCI DSS compliant helps protect customers' valuable card data.

> Merchants avoid expensive credit card non-compliant fees and possible legal issues from security breaches.

> Being PCI DSS compliant means merchants are exhibiting best practices to prevent cardholder information breaches.

> While PCI DSS compliance is not a guarantee of security, it is an important step in fraud prevention.

If your business fails to comply with PCI DSS, you risk substantial fines—


and even the loss of the ability to accept credit cards. Because of this, it is important that you become familiar with the specific PCI DSS validation requirements that apply to your business. These validation requirements vary according to the number of transactions an organization processes annually.

When you become PCI DSS compliant, you protect your customers from losing card data and safeguard yourself from possible legal issues and certain fines from the credit card companies.

**Validating PCI Compliance**

Acceptance of credit cards for payment has grown exponentially at small businesses across the U.S. Merchants of all sizes should be aware of the risk for theft and fraud, and take action to combat this by certifying with the industry standard for handling credit card data, called the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS validation is required for all businesses accepting credit cards.

**What does a merchant need to do to validate PCI DSS Compliance?**

There are two components required to validate or "prove" that a business has achieved PCI DSS compliance certification:

**1 Self-Assessment Questionnaire:**
All businesses are required to self-assess their IT and payment processing environment using the appropriate PCI DSS Self-Assessment Questionnaire (SAQ).

**2 Vulnerability Scanning:**
Depending on how you process payments and the Internet connection, network vulnerability scanning may also be required. (This step requires an Approved Scanning Vendor (ASV).

The questionnaire and the scanning will help identify if any weaknesses or vulnerabilities exist in the network. These issues must be fixed before PCI DSS certification can be achieved. Validation with PCI DSS is achieved with both a compliant, passing questionnaire and if necessary for your business, a compliant, passing vulnerability scan.

**How to get started:**

There are many tools available in the marketplace to help small merchants achieve these steps easily.

8818 Maxwell Drive, Suite 300
Potomac, Maryland 20854

T: 240-821-6900
F: 301-299-3618

info@summit-strategies.com
www.summit-strategies.com

Summit Strategies Merchant Services utilizes Security Metrics to provide validation services at a preferred price. Security Metrics is a leading provider of compliance and information security to the payment industry, serving merchants of all sizes. Security Metrics is used by the largest processors in the country and is certified to validate organizations' compliance with the PCI DSS.

## PCI DSS FAQ'S

### What is PCI DSS and to whom does PCI DSS apply?

The Payment Card Industry Data Security Standard (PCI DSS) was established by Visa, MasterCard, Discover, and American Express in order to create a set of standards and procedures for merchants to follow in order to protect sensitive cardholder information. Whether you are a small restaurant accepting cards with only a single terminal or you are a Fortune 500 company with hundreds of thousands of payment card customers and an advanced computer network, the PCI DSS applies to you.

### What is my next step to validate that I am PCI DSS Compliant?

The majority of merchants will only need to complete a PCI DSS Self Assessment Questionnaire (SAQ) that is available online via Summit Strategies Merchant Services preferred Qualified Security Assessor, Security Metrics. Those merchants that do not use terminals, but rather use POS software to process their payment cards will likely need to answer an expanded SAQ and also subject their business to a PCI DSS External Vulnerability Scan (Network Scan).

### How do I know what SAQ I need to answer and how do I know if I need to submit to a PCI DSS External Vulnerability Scan (Network Scan)?

If you are only using payment card terminals and are not storing card data electronically, then you will likely not require a PCI DSS External Vulnerability Scan (Network Scan) and will only need to answer the abbreviated SAQ. If you are using software, however, and your software is installed on a computer with access to the Internet, then you should visit Security Metrics Website at **https://securitymetrics.com** for more instructions regarding PCI DSS or you may speak to a Security Metric's representative.

### How long is the PCI DSS compliance certification valid?

The length of time a PCI DSS compliance certificate is valid depends on whether your business requires a SAQ and, where applicable, an external vulnerability scan. If your business requires only the SAQ, the PCI DSS certification is valid for one year. If your business also requires quarterly scans, the PCI DSS certification is valid for three months, at which time your next quarterly scan will be due.

### I process only a few hundred dollars a month. Does my merchant account still need to be PCI DSS compliant?

Yes. The Associations (Visa, MasterCard, American Express and Discover) have collectively adopted the PCI DSS as the requirement for businesses that process, store or transmit payment cardholder data, no matter how many cards are processed. Inherent in having a merchant account is the ability to appropriately handle cardholder data.

### Can I choose not to become PCI DSS compliant?

No. The Associations require all processors, like PNC Merchant Services, to report on the PCI DSS compliance status of their merchants. If you choose not to complete the SAQ, you may overlook certain data security practices that could increase your risk of a security breach. In the event that your business is compromised, you may be subject to fines from each Association. These fines would be in addition to the expenses and fraudulent transactions resulting from the breach.

(*Information provided by First Data Merchant Services*)