

# PCI Compliance

## Top 10 Questions & Answers

1. What is PCI Compliance and PCI DSS?
2. Who needs to follow the PCI Data Security Standard?
3. What happens if I don't comply?
4. What are the basic requirements of PCI compliance?
5. How do I validate PCI DSS compliance?
6. How does my Acquiring Bank fit in?
7. How do I get started?
8. What else can I do to minimize risk?
9. What happens when I am PCI DSS certified?
10. What can CompliancePoint do for me?

### **1. What is PCI Compliance and PCI DSS?**

PCI (Payment Card Industry) DSS (Data Security Standard) is a security standard developed by the PCI Council for all merchants who accept and process credit cards. The standard is validated either quarterly or annually by a merchant and the validation of compliance is then reported to a merchant's Acquirer.

The number of security breaches is increasing. In one recent incident, hackers compromised more than \$45 million in credit and debit cards. This type of incident has made it necessary to protect consumer identities and company brands through stronger protection of cardholder data.

The credit card associations responded to this growing threat by joining together in 2005 and creating the PCI Council. The Council consists of the 5 major credit card brands: VISA, MasterCard, American Express, Discover Card, and JCB International. The group created the PCI DSS and the PCI Council now requires merchants to follow this standard to help protect credit card information from malicious attack.

More information on the standard can be found at: <http://www.pcisecuritystandards.org>.

## **2. Who needs to follow the PCI Data Security Standard?**

The simple answer is, every merchant does. The standard is mandatory for all merchants who accept credit cards, and provides a best practice framework for securing sensitive information. Merchants who accept credit card payments are liable if information is compromised through their business.

This means that in the event of an information compromise, your business can be fined by the card associations and you can lose your merchant account. By complying with the PCI DSS and validating the compliance of your business, you greatly reduce the chances of this happening.

The requirements for validating the compliance of your business vary based on the size of your business (*see Table 5a of this guide, Merchant Compliance Levels*). All merchants are required to validate their compliance on a yearly and sometimes on a quarterly basis.

## **3. What happens if I don't comply?**

Current fines range from \$90-\$305 per compromised record and up to \$500,000 per incident (Forrester Research) if your network is determined to be non-compliant when it suffered a breach that resulted in the loss or theft of cardholder information.

Even if there is not an actual loss of information from a breach, a company that is non-compliant can lose its ability to accept credit cards.

## **4. What are the basic requirements of PCI compliance?**

Many large data losses arise from a lack of physical and internal controls that provide external hackers with a means to access cardholder data. PCI DSS creates a standard to help prevent the loss of this data. This standard comprises 6 general "areas" of requirements.

**Table 4 - Summary of PCI DSS Requirements**

Area	Requirement	Details
<b>Build &amp; Maintain A Secure Network</b>	<p><b>Requirement 1:</b> Install and maintain a firewall configuration to protect cardholder data</p> <p><b>Requirement 2:</b> Do not use vendor-supplied defaults for system passwords and</p>	<p>Firewalls are computer devices that control computer traffic allowed into and out of a company's computer network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.</p> <p>All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are an important protection mechanism for any computer network.</p>
<b>Protect Cardholder Data</b>	<p><b>Requirement 3:</b> Protect stored cardholder data</p> <p><b>Requirement 4:</b> Encrypt transmission of cardholder data across open, public networks</p>	<p>Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending PAN in unencrypted e-mails. Sensitive information must be encrypted during transmission over networks that are easy and common for a hacker to intercept, modify, and divert data while in transit.</p> <p>Encryption is a critical component of cardholder data protection. Even if an intruder is able to circumvent other network security controls and gain access to encrypted data, he or she would need the proper cryptographic keys to read and use the data.</p>
<b>Maintain A Vulnerability Management Program</b>	<p><b>Requirement 5:</b> Use and regularly update anti-virus software or programs</p> <p><b>Requirement 6:</b> Develop and maintain secure systems and applications</p>	<p>Many vulnerabilities and malicious viruses enter the network via employee e-mail activities. Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software. Unscrupulous individuals use security vulnerabilities to gain privileged access to systems.</p> <p>Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses.</p> <p>For in-house developed applications, multiple vulnerabilities can be avoided by using standard system development processes and secure coding techniques.</p> <p>Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations.</p>
<b>Implement Strong Access Control Measures</b>	<p><b>Requirement 7:</b> Restrict access to cardholder data by business need-to-know</p> <p><b>Requirement 8:</b> Assign a unique ID to each person with computer access</p> <p><b>Requirement 9:</b> Restrict physical access to cardholder data</p>	<p>Create and implement policies that ensure only employees that require information have access to data.</p> <p>Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.</p> <p>Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.</p>
<b>Regularly Monitor &amp; Test Networks</b>	<p><b>Requirement 10:</b> Track and monitor all access to network resources and cardholder data</p> <p><b>Requirement 11:</b> Regularly test security systems and processes</p>	<p>Logging mechanisms and the ability to track user activities are critical. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs. Vulnerabilities are continuously being discovered by hackers and researchers and exploited by new software.</p> <p>Systems, processes, and custom software should be tested frequently to ensure security is maintained over time and with any changes in software.</p>
<b>Maintain An Information Security Policy</b>	<p><b>Requirement 12:</b> Maintain a policy that addresses information security for employees and contractors</p>	<p>A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibility to protect it.</p>

## 5. How do I validate PCI DSS compliance?

Merchants are divided into four different levels based on the number of credit card transactions they process annually. These levels determine the type of PCI validation required (*see Table 4 of this guide above, PCI DSS Merchant Compliance Levels*).

To summarize, Level 1 merchants are required to conduct an on-site audit once a year, and implement quarterly network scans.

Merchant Levels 2 and 3 are required to validate compliance through an annual Self Assessment Questionnaire (SAQ) and quarterly network scans. The SAQ is either provided by your acquirer or can be downloaded from the PCI Council's website (<http://www.pcisecuritystandards.org>).

Level 4 merchants are also required to validate compliance through an annual Self Assessment Questionnaire and some are required to run a quarterly scan (*see Tables 5a and 5b of this guide for more information*).

If you experience a security breach that results in the loss or theft of cardholder information, you are automatically treated as a Level 1 merchant.

Merchant Level	Description	Compliance Validation	Validate By
1	Over 6,000,000 transactions per year; or  Any Merchant that has suffered an attack causing account data to be compromised.	Annual on-site security audit;  Quarterly network scan*	Approved Independent security assessor; or Internal audit,  Approved Independent Scan vendor
2	150k to 6,000,000 transactions per year	Annual self assessment;  Quarterly network scan	Merchant;  Approved Independent Scan vendor
3	20k to 150k transactions per year	Annual self-assessment;  Quarterly network scan	Merchant;  Approved Independent Scan vendor
4	Less than 20k transactions per year	Annual self-assessment**	Merchant;  Approved Independent Scan vendor

**\*Quarterly Network Scan.** CompliancePoint has partnered with ControlScan to provide you with a solution for your quarterly network validation scan. ControlScan is an Approved Scanning Vendor (ASV) and has one of the industry's most complete security vulnerability assessment capabilities.

**\*\*Annual Self Assessment.** For Level 4 merchants, CompliancePoint makes the annual process easy by providing you with an online, hosted, Self-Assessment Questionnaire, so you don't need to submit the questionnaire to us

To complete the SAQ, you will need to choose 1 of the 4 types of questionnaires. Use table 5b to review the description and select the right SAQ.

**Table 5b - SAQ Forms By Transaction Type**

Description	SAQ Form
Card-not-present (e-commerce or mail/telephone-order) merchants with all cardholder data functions outsourced. This does not apply to face-to-face merchants. Merchants offering cardnot-present transactions retain only paper reports or receipts with cardholder data, do not store cardholder data in electronic format, and do not process or transmit any cardholder data on their premises.	<b>A</b>
Imprint-only merchants with no electronic cardholder data storage	<b>B</b>
Stand-alone terminal merchants with no electronic cardholder data storage	<b>B</b>
Merchants with POS systems connected to the Internet, no electronic cardholder data storage	<b>C</b>
All other merchants (not included in Types 1-4 above) and all service providers defined by a payment brand as eligible to complete an SAQ. Electronic cardholder data is stored.	<b>D</b>

### 6. How does my Acquiring Bank fit in?

An acquiring bank underwrites your credit card activity and provides you with a merchant account through which to process your credit card transactions. The acquiring bank has a direct relationship with you, and is responsible for monitoring your PCI compliance status. Quarterly scan validation and the yearly Self-Assessment Questionnaire are presented to the acquiring bank, which in turn provides updated validation status information to MasterCard and Visa. If you are out of compliance and experience fines, the fines are passed through your acquiring bank to you.

### 7. How do I get started?

For those who have limited knowledge about security, the PCI DSS requirements may seem daunting. We've outlined the 5 key steps below to make it easier for you to ensure you are in compliance. The PCI DSS requirements reflect the minimum security you need to ensure compliance, so as the business manager, you should understand your transaction and storage processes to determine if this level of security meets your unique business needs.

Before you start, take some time to review each of the following requirements to understand how it is or how it could be implemented in your network. If at any time you answer no to a requirement, you will need to either resolve it or put in place a mitigating control that alleviates the issues that non-compliance would cause. The mitigating control must have a timeline that defines when the control will be removed and a solution put in place.

- A. Understand all of your sales channels that take credit card payments and how that payment information is processed, transmitted and stored.
- B. Determine if any of your sales channels are hosted by another third party or by yourself. If you are using a third party, you will need to get confirmation that the third party is PCI DSS certified. The third party will often assume the responsibility for implementing some of the PCI DSS requirements, but you will still be responsible for validating the compliance of your business.
- C. Understand the scope of PCI DSS. You are required to run a quarterly scan on your network if you process, transmit or store information on that network and the network interacts with the Internet. Determine the network and the IP addresses that will be used to validate PCI DSS compliance. PCI DSS applies to all "system components," which are defined as any network component,

server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Adequate network segmentation\*, which isolates systems that transmit, store, access or process cardholder data from those that do not, may reduce the scope of risk of the cardholder data environment.

- D. Once you confirm that the requirements are in place, you will be ready to complete the Self-Assessment Questionnaire and, if applicable, run a network vulnerability scan (from an ASV – Approved Scanning Vendor). If you do not pass the scan, work through the vulnerabilities and correct them. If you are a Level 1 merchant, you will be required to retain a QSA (Qualified Security Assessor) to review and audit your compliance to the PCI DSS standard instead of the annual self-assessment questionnaire.
- E. Send PCI compliance validation to your Acquiring Bank as requested, and directly to American Express, Discover and JCB.

## **8. What else can I do to minimize risk?**

One of the easiest ways to minimize your risk of non-compliance and theft of cardholder data is to limit the amount of customer data you handle and store. If you do not use the information, do not store the data. If you work with providers who handle the payment data and storage, your risk is significantly reduced.

## **9. What happens when I am PCI DSS certified?**

Your acquirer or PCI security provider will notify you once you have been certified. Remember that PCI DSS is a best practice guide to ensure that credit card data is stored, processed and transmitted securely, so you need to ensure that the requirements are consistently and continuously implemented.

Once you are certified, you are required to complete an annual Self-Assessment Questionnaire. If your business systems require a scan, this must be done on a quarterly basis. If you are a Level 1 merchant, you will be required to retain a QSA (Qualified Security Assessor) to review and audit your compliance to the PCI DSS standard instead of the annual Self Assessment Questionnaire.

## **10. What can CompliancePoint do for me?**

CompliancePoint is a leading provider of industry and regulatory compliance services including the two main PCI standards, PCI DSS and PA-DSS. The CompliancePoint approach assists the customer through all three phases of the PCI project (Gap Analysis, Remediation, and Final Audit).

In addition, the customer has use of the CompliancePoint Project Management Portal for the entire project, giving multi-level visibility of the project tasks, milestones, assignments and outstanding items. It also acts as an excellent repository and communication vehicle for the project team and executive sponsors. CompliancePoint is focused on getting the customer certified and, to that point, offers a fixed price approach for the entire process — whether it takes 8 weeks or 8 months, the price does not change. If time is the biggest issue for the project, remediation services are available to assist, augment or outsource some or all of the remediation requirements.