

# Payment Card Industry Data Security Standard- PCI DSS

## Executive Summary

### PCI Compliance: Business Owners / IT Managers Guide

PCI Standards must be met by all businesses that take credit/debit or pay cards from the top four major card industry providers: American Express, Discover, MasterCard and Visa. PCI Compliance Standards are not laws – they are contractual obligations with the credit card companies. Credit card companies may enforce the terms of their contracts by imposing fines and/or sanctions against companies who do not comply with the standards for each credit card company.

### What is Payment Card Industry (PCI) Compliance?

Payment Card Industry (PCI) Compliance is a set of security standards that were created by the major credit card companies (American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International) to protect their customers from increasing identity theft and security breaches. Under the PCI DSS, a business or organization should be able to assure their customers that its credit card data/account information and transaction information is safe from hackers or any malicious system intrusion.

### Do I need to become compliant?

Any company that accepts, processes, or stores credit card information needs to comply with the standards set by the Payment Card Industry. This includes POS software vendors, 3<sup>rd</sup> party service providers, merchants of all types, and any other entity who is part of the payment transaction process.

### What are my requirements for PCI Compliance?

The requirements for becoming Payment Card Industry (PCI) Compliant are dependent upon the merchant level that a company falls under. Merchants are divided into four different levels based on the number of transactions they process throughout a year.

#### Level 1 Criteria

Merchants with over 6 million transactions a year  
Merchants whose data has been compromised

#### Level 1 Requirements

Annual Onsite Security Audit and quarterly network security scan

#### Level 2 Criteria

Merchants with 150,000 to 6 million transactions a year

**Level 2 Requirements**

Annual Self Assessment Questionnaire  
Quarterly Scan by an Approved PCI Scanning Vendor

**Level 3 Criteria**

Merchants with 20,000 to 150,000 transactions a year

**Level 3 Requirements**

Quarterly Scan by an Approved PCI Scanning Vendor  
Annual Self Assessment Questionnaire

**Level 4 Criteria**

Merchants with less than 20,000 transactions

**Level 4 Requirements**

No need to report compliance but must maintain compliance.

**What kind of a scan needs to be performed?**

Vulnerability Assessment Scans must be performed by Payment Card Industry Approved Scanning Vendors (ASV). The scan will be performed over all externally facing IP addresses that touch the credit card acceptance, transmission and storage process. Scans must be turned into the merchant bank on a quarterly basis.

**How do I report compliance?**

Both the passing PCI Scan and Annual Self Assessment Questionnaire should be turned into your merchant bank. Your merchant bank will then report back to the Payment Card Industry that your company is PCI Compliant.

**What happens if I am not compliant?**

Failure to comply with the Payment Card Industry security standards may result in heavy fines, restrictions, or permanent expulsion from card acceptance programs.

Card companies may impose fines on their member banking institutions when merchants are found to be non-compliant with PCI DSS. Acquiring banks may in turn contractually oblige merchants to indemnify and reimburse them for such fines. Fines could go up to \$500,000 per incident if data is compromised and merchants are found to be non-compliant. In the worst case scenario, merchants could also risk losing the ability to process customers' credit card transactions.