

securityMETRICS

PAYMENT CARD INDUSTRY
DATA SECURITY STANDARDS

MERCHANT COMPLIANCE GUIDE

Copyright© 2005
SecurityMetrics

Merchant
Compliance

Merchant Security Compliance—**What is it?**

What is it?

Rising Problem of Identify Theft

The increased use of the Internet has caused a rise in the electronic theft of credit card information from merchants. Many fraudulent card transactions are directly connected to identity theft from another merchant. These incidents reduce consumer confidence and increase costs to consumers, merchants and their supporting banks.

Does it apply?

What is required?

The increase in identity theft has prompted the credit card associations (American Express, MasterCard, Visa and Discover) to establish security requirements for merchants. Compliance with these requirements will increase consumer confidence while reducing identity theft and fraud.

Scan
Guidelines

Card Association Security Programs

The card associations have established the Payment Card Industry Data Security Standard (PCI DSS) for merchants. All major card associations have endorsed this program.

Enforcement of these standards varies among the card associations. Visa & MasterCard rely on acquiring/member banks to enforce compliance among merchants.

Consequences of non-compliance include: fines, expensive recovery costs, and/or the loss of a merchant's ability to accept card transactions. These consequences are being applied to organizations that ignore compliance deadlines or experience card data compromise, regardless of deadline dates.

Merchant
Compliance

Does this Apply to My Merchant Business?

What is it?

Does it apply?

What is required?

Scan
Guidelines

Storing, Processing, or Transmitting Cardholder Data?

Every merchant that “stores, processes or transmits” card holder data electronically is affected by the PCI Data Security Standards (PCI DSS). It is important to realize that this is **not** only an e-commerce standard.

All Merchants

By definition, a card transaction means that a merchant is transmitting data electronically, thus, all merchants have a responsibility to insure PCI DSS compliance.

The extent of each merchant's compliance requirements varies depending on the volume of cards processed, handled or transmitted and the transaction tools used by the merchant.

But I Use a Service Provider for My Transactions

Many merchants have felt that their use of a third party service provider removes them from the PCI DSS requirements. A merchant's use of a third party provider, hosting company, gateway, etc. does not remove the responsibility from the merchant to insure compliance.

“If there are service providers handling cardholder data on an entity’s [merchant’s] behalf, the entity must ensure that contracts with these service providers specifically include CISP [PCI DSS] compliance as a condition of business.”

FAQ.pdf as provided by Visa for the PCI DSS

Merchant Compliance

What is it?

Does it apply?

What is required?

Scan Guidelines

What Is Required Of My Merchant Business?

The PCI DSS program determines the compliance requirements based on the transaction type and volume. Please review the table below to determine your organizations' compliance requirements.

On-Site PCI DSS Audits

These audits require an extensive review of the merchant's card processing infrastructure, security practices, tools and policies. If your organization must meet this requirement, please contact SecurityMetrics for a quote

Scans

The Quarterly or Annual Scan requirement states: "A quarterly or annual system perimeter scan must be performed on the merchant's external-facing IP addresses".

This security

test is commonly referred to as a Vulnerability Assessment and uses hacker techniques to discover security weaknesses in your computers, servers, and/or networks. The tests are non-disruptive to computer operations.

Assistance in determining the extent of your "external-facing IP addresses" is provided in this guide. You can also contact SecurityMetrics for assistance. Merchants are compliant with this requirement when they are testing all the required IP addresses/URLs and each is receiving a passing status.

Self-Assessment Questionnaire

Merchants are expected to achieve a passing grade on the Self-Assessment Questionnaire in order to achieve a certified status.

SecurityMetrics Role

SecurityMetrics is authorized to perform the security scans. The SecurityMetrics scans are accurate and easy to understand. The SecurityMetrics Site Certification service includes the initial tests, unlimited retesting (if needed), and friendly help-desk support. Your appropriate self-assessment questionnaire is available online and automated reporting to your authorized acquiring bank is provided.

Merchant Levels & Compliance Requirements

Level	Qualification Criteria	Security Requirements
1	Any merchant processing over 6,000,000 Visa or MasterCard transactions per year.	* On-Site PCI DSS Audit * Quarterly Scan
2 & 3	Any merchant processing 20,000 to 6,000,000 Visa or MasterCard e-commerce transactions per year.	* Quarterly Scan * Self-Assessment Questionnaire
4	All other merchants	* Annual Scan * Self-Assessment Questionnaire

Merchant
Compliance

Scan Guidelines

What is it?

The general PCI DSS guideline regarding scanning states that security testing is to be performed against all “Internet-facing perimeter systems”. The detailed guidelines mention web servers, virtual hosts, email servers, DNS servers, firewalls, routers, application servers, and especially custom-developed e-commerce applications.

Does it apply?

What is required?

http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Security_Scanning_Procedures.pdf

Scan Guidelines

Merchants typically have three areas to consider: 1) Business Networks 2) Home Computers and 3) Ecommerce.

Business Networks typically have some or all of the devices mentioned above. The merchant needs to determine the extent of their external exposure (IP addresses that are public, not private). If your business hosts its own ecommerce, identification and testing of all your public IP addresses should suffice.

Home Computers can be a bit more challenging. SecurityMetrics has solutions for testing dynamic public IP addresses which occur with many home internet connections.

Ecommerce systems are usually divided between general marketing, a shopping cart and a secure purchase page. These functions may reside on any combination of actual servers. The merchants’ responsibility is to ensure that they are all certified, either by testing them all, and/or by obtaining proof of certification from the service providers.

Please Note: If these functions are handled by different servers, a common misconception is to only scan the server hosting the secure purchase page. The logic is that, “it is the only server handling customer card data”. Merchants need to know that the PCI DSS requirements do not make such an exclusion of the servers hosting marketing or shopping cart functionality.

Most merchants are unaware of the many incidents of card abuse and theft due to the marketing and shopping cart servers being hacked. For example, these incidents have allowed hackers to:

- 1) Steal secure codes from the merchant’s marketing server which led to unauthorized access of the merchant’s transaction data from their gateway/processor.
- 2) Insert fake purchase pages into the merchant’s purchase process, thus tricking customers into providing card data prior to the normal “secure” purchase page.

Information-Only Web Sites also present a vehicle for fraud and card abuse. Keeping these sites secure with periodic scans is important to protect the published phone numbers, fax numbers and email addresses for purchases. Hackers have been known to change contact information to collect credit card data from unsuspecting customers.
