White Paper

AppLabs
no doubt about it

PCI DSS Compliance

An Overview

Last Updated: 21st August, 2007

Introduction

The growth of online services to facilitate ease of use for customers to purchase goods has grown exponentially over recent years. In order to make this process easier, customers generally pay for the services or goods by credit or debit card. However, improved efficiency and convenience for the consumer mean crime has also become easier and more convenient.

Criminals have become more skillful having discovered that there is a significant amount of money to be acquired with very little risk and as such, credit card fraud and identity theft have become much more common place in recent years. Network infrastructures that are utilized commercially necessitate absolute security due to the sensitive personal information which they contain.

Every company that accepts credit card payments, processes credit card transactions, stores credit card data, or in any other way touches personal or sensitive data associated with credit card payment processing, is affected by PCI DSS.

What is PCI DSS?

Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards that has been 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.

Who must comply with PCI DSS?

Virtually all businesses, regardless of their size, need to understand the scope of PCI DSS and how to implement network security that is compliant with PCI DSS guidelines. In doing so, they will avoid penalties or the possibility of having their merchant status revoked and potentially being banned from accepting or processing credit cards.

Any company that stores, processes or transmits cardholder data must comply with PCI DSS. Primarily, merchants and service providers should be compliant to this standard. Merchants are the companies that accept credit cards in exchange for goods or services. A service provider is any company that processes, stores, or transmits cardholder data, including companies that provide services to merchants or other service providers. To comply with this standard a merchant or service provider has to satisfy the requirements listed below.

Overview of PCI DSS Requirements

PCI DSS version 1.1 comprises six control objectives which in turn contain one or more requirements covering the ambit of IT security with a mix of technical and security controls. According to PCI DSS 1.1, the scope includes the cardholder data environment only if adequate network segmentation is in place. In most cases, this implies the use of dedicated firewalls and non-routable virtual local area networks (VLANs). If you do not have such controls in place, the scope of PCI compliance validation will cover your entire network. The list below elucidates the 12 PCI requirements:

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks
- Requirement 5: Use and regularly update anti-virus software
- Requirement 6: Develop and maintain secure systems and applications
- Requirement 7: Restrict access to cardholder data on a need-to-know basis
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data
- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes
- Requirement 12: Maintain a policy that addresses information security

Compliance Process

Depending on the company's merchant or service level provider, either an annual onsite PCI audit has to be conducted, or a Self-Assessment Questionnaire (SAQ) has to be filled in to validate compliance. In addition to this, results of quarterly network perimeter scans (which have to be performed by an approved scanning vendor), evidence of internal vulnerability scans and evidence of application and network penetration tests are to be shared with card brands to prove to them that the company practices sound patch management and vulnerability management processes.

PCI classifies merchants and service providers based on the number of transactions that take place through their service. Table I and II below classifies different levels for a merchant and service providers.

Level	Selection Criteria	Compliance
Level 1	More than six million VISA/Mastercard transactions annually across all channels, including e-commerce	▸ Annual onsite PCI data security assessment ▸ Quarterly network scans
Level 2	1,000,000 - 5,999,999 VISA/Mastercard transactions annually	▸ Annual self-assessment ▸ Quarterly network scans
Level 3	20,000 - 1,000,000 VISA/Mastercard e-commerce transactions annually	▸ Annual self-assessment ▸ Quarterly network scans
Level 4	Less than 20,000 e-commerce transactions annually and all merchants across channel up to 1,000,000 VISA transactions annually	▸ Annual self-assessment ▸ Annual network scans

Level	Selection Criteria	Compliance
Level 1	All VisaNet processors (member and nonmember) and all payment gateways	▸ Annual onsite PCI data security assessment ▸ Quarterly network scans
Level 2	Any service provider that is not in Level 1 and stores, processes or transmits more than 1,000,000 VISA/ Mastercard accounts/transactions annually	▸ Annual onsite PCI data security assessment ▸ Quarterly network scans
Level 3	Any service provider that is not in Level 1 and stores, processes or transmits fewer than 1,000,000 VISA/ Mastercard accounts/transactions annually	▸ Annual self-assessment ▸ Quarterly network scans

Achieving PCI DSS Compliance

It is recommended that a proactive means for merchants and service providers to meet PCI DSS compliance is by having their network perimeter scanned by an Approved Scanning Vendor (ASV) every quarter. An ASV, on request of merchant or service provider shall obtain required information, run a scan and submit a scan report clearly highlighting compliance status, network vulnerabilities and vulnerable services classified as per the scoring pattern and severities prescribed by PCI DSS. The compliance scan follows the steps highlighted below:

- The Merchant or Service Provider engages with ASV to perform the PCI DSS scanning service;
- The Merchant provides ASV with information about their network perimeter. Any special requirements like exclusion or justification of specific services are taken into account as part of this step;
- The ASV scans merchant's network perimeter from a remote site using non-intrusive tests;
- The ASV determines compliance based on the vulnerabilities found during the assessment. This is benchmarked against the scoring matrix provided by PCI DSS;

- The ASV produces a report containing the PCI DSS status of each scanned network component with recommendations to address the vulnerabilities;
- The ASV and the merchant shall review the vulnerabilities together and apply suggested fixes to mitigate any perceived risk and maintain compliance to PCI DSS.

Benefits of Compliance

- By complying with PCI DSS, the organization has taken the appropriate steps to ensure that its customers and their data are secure;
- One of the benefits of PCI DSS compliance is that the organization will not face a severe penalty if their services are breached. If the analysis after a security incident shows that the company was still compliant at the time of the incident this will be treated with leniency by the authorities;
- More importantly, if your company is a Level 1 or Level 2 merchant, you may be eligible to receive part of the $20 million in financial incentives from Visa;
- By obtaining PCI DSS compliance status it will attract discounts on transaction costs from the credit card companies.