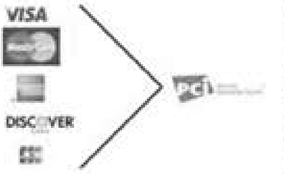
Payment Card Industry Data Security Standard (PCI DSS): Made Easy Easy

Mohammad Tohidur Rahman Bhuiyan

PCI SSC & PCI DSS

The PCI Security Standards Council, which I'll refer to as "the Council" or "PCI SSC" going forward, is an independent industry standards body that develops and manages the payment card industry security standards on a global basis. The PCI SSC consists of five founding payment brand members: American Express, Discover, JCB International, MasterCard, and Visa. They maintain a very high level of support and are very active in the PCI Council and the direction we are taking.



Overview of PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is mandatory compliance program resulting from a collaboration between the credit card associations. It is a widely accepted multifaceted and actionable security standard/ framework that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard (common industry security baseline of technical & operational requirements and Common auditing & scanning procedures) is intended to optimize the security of credit, debit and cash card transactions and proactively protect (Enables prevention, detection and appropriate handling/ reacting of security incidents) cardholders against misuse of their personal information for organizations that handle branded credit cards from the major card brands including Visa, MasterCard, American Express, Discover, and JCB.

PCI DSS Goals and Functional Requirements :

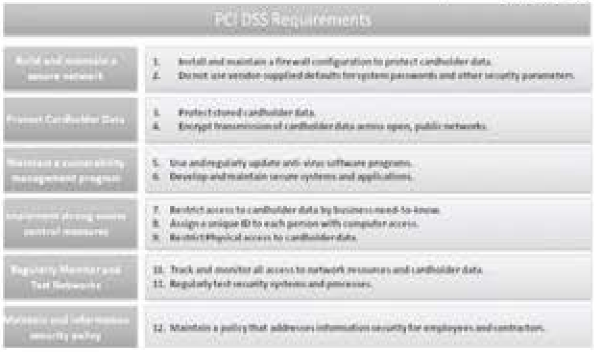
PCI DSS includes 6 Goals and 12 functional Requirements (detailed over 240 requirements) based on -

* Administrative controls (policies, procedures, etc.)

* Physical security (locks, physical barriers, etc.)

* Technical security (passwords, encryption, etc.)

*** Summary of PCI DSS Requirements (mapping with its Goal)**



PCI DSS Requirements	
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software programs. 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know. 8. Assign a unique ID to each person with computer access. 9. Restrict Physical access to cardholder data.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors.

Merchant Level, Responsibilities and Validation

Achieving and maintaining compliance with the PCI DSS is a difficult proposition for many organizations. The specificity of the required controls, and the processes and procedures required to demonstrate that the controls are managed in a secure manner requires a significant outlay of capital and resources for companies pursuing compliance.

It is common for merchants to be contacted by their acquirer and told that they need to achieve PCI DSS compliance. These communications tend to go out to clients that have some form of merchant services capability. This will usually be through mail order Telephone Order (MO/TO), card not present, or face to face card processing requirements.

Merchants are instructed to complete either Self-Assessment-Questionnaires (SAQ) or Reports on Compliance (ROC). This requirement is determined by the number of transactions that an organization processes each year.

In addition, any merchant with e-commerce must also complete a vulnerability scan by an Approved Scanning Vendor (ASV).

Listed in a generalized format, are the different levels and requirements of a merchant regarding PCI DSS.

American Express does not use the format listed above. Please refer to their website for information on their definitions and requirements: americanexpress.com

Note:

If a breach has been reported, or found, Payment Brand e.g. VISA, MasterCard reserves the right to move the Level 4 merchant to a Level 1. If so, the Level 4 merchant must abide by

Level	Definition	Requirements
1	Processes over 6 million transactions annually	Annual on-site audit by a QSA Quarterly scans for network vulnerability by an ASV
2	Processes 1 million to 6 million transactions	Annual on-site self-assessment.
3	Processes 20,00 to 1 million transactions annually	Annual on-site self-assessment. Quarterly scans for
4	All other merchants	Annual on-site self-assessment. Quarterly scans for

the Level 1 validation requirement.

A merchant meeting Level 1 criteria in any country/region that operates in more than one country/region is considered a global Level 1 merchant. Exceptions may apply to global merchants if no common infrastructure exists or if Visa data is not aggregated across borders; in such cases the merchant validates according to regional levels.

In addition to adhering to the PCI Data Security Standard, compliance validation is required for Level 1, Level 2, and Level 3 merchants, and may be required for Level 4 merchants.

Compliance

Compliance means **adherence** to the standard -

Applies to -

* PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities regardless of size or number of transactions, that "stores, process, or transmit cardholder data" and/or sensitive authentication data.

* all payment (acceptance) channels, including brick-and-mortar, mail, telephone, e-commerce (Internet),POS, IVR etc. and

* All Paper based transaction.

Even if any customer of that organization ever pays the merchant directly using a credit card or debit card, then the PCI DSS requirements apply.

* Technical and business practices

PCI DSS Phases & Deliverable

PCI DSS's 12 requirements specify the framework for a secure payments environment; for purposes of PCI compliance, their essence is three steps: Phase One – Discovery & Analysis, Phase Two – Remediation Activities and Phase Three – Report.

* **Assess** is to take an inventory of your IT assets and business processes for payment card processing and analyze them for vulnerabilities that could expose cardholder data.

* **Remediate** is the process of fixing those vulnerabilities.

* **Report** entails compiling records required by PCI DSS to validate remediation and submitting compliance reports to the acquiring bank and global payment brands you do business with.

Carrying out these three steps is an ongoing process for continuous compliance with the PCI DSS requirements. These steps also enable vigilant assurance of payment card data safety.

Attestation

Letter to Payment Brand e.g. VISA signed by both merchant and acquirer bank attesting that validation has been performed.

Why Comply with PCI Security Standards?

Compliance with data security standards can bring major benefits to businesses of all sizes, while failure to comply can have serious and long-term negative consequences. Here are some reasons why.

Compliance with the PCI DSS means that your systems are secure, and customers can trust you with their sensitive payment card information.

Compliance improves your reputation with acquirers and payment brands — the partners you need in order to do business.

Compliance is an ongoing process, not a one-time event. It helps prevent security breaches and theft of payment card data, not just today, but in the future.

As indirect benefit, you'll likely be better prepared to comply with other regulations as they come along, such as ISO 27001, ISO 20000, ISO 9001 and HIPAA, SOX, etc.

Breach, Risk and Consequences

A single retailer, or merchant, can process millions payment card transactions each year. If an unauthorized route is found into that merchant's system then the potential for fraudulent use of credit and debit card details is huge.

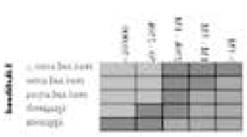
Reputation Risk

* What will the impact be on your company's brand?

* Mandatory involvement of federal law enforcement in investigation

Financial Risk

* Merchant banks may pass on substantial fines



* Up to $500,000 per incident from Visa alone

* $20 - $90 fine per credit card number that COULD have been exposed or compromised

* Civil liability and cost of providing ID theft protection

* Average cost of a security breach is $5,000,000

Compliance Risk

* Exposure to Level 1 validation requirements

Operational Risk

* Visa imposed operational restrictions

* Potential loss of card processing privileges

PCI DSS in Bangladesh

In the US there are states that have state laws in place which force components of PCI DSS. It has been noted that the Bangladesh government and regulatory authorities are generally getting more active in the area of data protection. Central Bank of Bangladesh (Bangladesh Bank) is fully aware of PCI DSS Compliance by PCI SSC (American Express, Discovery, Master Card, VISA & JCB) and "Private Label Cards" (those without a logo from a major card brand which are not included in the scope of the PCI DSS). In sub clause 9.3.7 of Chapter 9, "Alternative Delivery Channels (ADC) Security Management" under "Guideline on ICT Security for Banks and NBFIs", Version 3.0 (May 2015) by Bangladesh Bank, PCI DSS Compliance is made as a **requirement**.

Summary

It is in everyone's interest – whether consumer, merchant or bank – that the standard is consistently enforced so that sensitive data is protected and the cost of fraud is minimized for all parties. Indeed many public organizations that store sensitive customer information (not necessarily specifically payment card data) will also benefit from adopting PCI DSS standards.

You've worked hard to build your business – make sure you secure your success by securing your customers payment card data. Your customers depend on you to keep their information safe – repay their trust with compliance to the PCI Security Standards.

Perhaps I made the hairs on the back of your neck stand up for a moment – but I am here to assist that can help. Take the first step in your PCI Security Standards compliance journey with a PCI DSS Compliance Validation Service Provider ■

Reference:

PCI SSC, Wikipedia, all contributors in www