

## **What are the Payment Card Industry (PCI) Data Security Standards?**

The PCI Data Security Standards are association (Visa/MasterCard) and industry mandated requirements for handling of credit card information, classification of merchants, and validation of merchant compliance. As a merchant, you are responsible for any damages or liability that may occur as a result of a data security breach or other non-compliance with the PCI Data Security Standards.

## **What are the requirements for PCI DSS?**

- 1.) *Build and maintain a secure network:* Install and maintain a firewall and use unique, high-security passwords with special care to replace default passwords.
- 2.) *Protect cardholder data:* Whenever possible, do not store cardholder data. If there is a business need, you must protect this data. You must also encrypt and data passed across public networks, including your shopping card and web-hosting providers.
- 3.) *Maintain a vulnerability management program:* Use an anti-virus software program and keep it up date. Develop and maintain secure operating systems and payment applications. Ensure the anti-virus software applications you use are compliant (see [www.visa.com/pabp](http://www.visa.com/pabp)).
- 4.) *Implement strong access control measures:* Access, both electronic and physical access, to cardholder data should be on a “need-to-know” basis. Ensure those people with access have a unique ID and password for electronic access. Do not share logon information.
- 5.) *Regularly monitor and test networks:* Track and monitor all access to networks and cardholder data. Ensure you have a regular testing schedule for security systems and processes: firewalls, patches, and anti-virus.
- 6.) *Maintain an information security policy:* It is critical that your organization has a policy on how data security is handled at your business. Ensure you have an information security policy and that it’s disseminated and updated regularly.

## **Is this a one-time requirement?**

No. PCI DSS compliance is an ongoing process. Validation actions vary depending on the actual number of transactions you process. However, credit card associations require all merchants to comply with PCI DSS at all times. There are two main components of validation:

- 1.) Completing the PCI Self-Assessment Questionnaire (SAQ) annually

- 2.) Undergoing network vulnerability scans performed by an approved scanning vendor quarterly.

## **Are all merchants and service providers required to comply with PCI DSS?**

Yes, Any entities (merchants or service providers) that store, or transmit cardholder data must comply with the PCI DSS. The requirements apply to all acceptance channels including retail (brick and mortar), mail/telephone order (MOTO) and e-commerce. Validation requirements vary depending on the number of transactions an entity processes.

## **What is a data compromise?**

A data compromise is an incident involving the electronic or physical breach of cardholder data through the communication and/or information processing of the merchant/third party. Electronic breaches include data vulnerability in transit or storage; attacks via websites or servers, private key mismanagement, access related to user ID or password, and administrative network performance problems. Physical breaches include theft of documents or equipment such as receipts, files, PCs, or POS terminals. Skimming breaches are actually a hybrid of both a physical and electronic breach as the perpetrator takes possession of the card, steals the magnetic stripe data and returns the card to the cardholder.

## **What are the benefits of being in compliance with PCI DSS?**

It is good business practice to adhere to the PCI standards and protect cardholder information. Additionally, Visa, MasterCard and Discover may impose fines on their member banking institutions when merchants do not comply with PCI DSS. You are contractually obligated to indemnify and reimburse the processor, as your acquirer, for such fines. Please note such fines could be significant (as much as \$500,000), especially if your business is compromised and you have not been validated as compliant.

## **How do I become PCI Compliant?**

If you need to know more and would like to speak to an individual specializing in helping merchants protect their card holder data, please email us your name and phone number and we will contact you.