**PCI DSS Validation Requirements**

**What is PCI DSS compliance?**

All merchants processing, transmitting, or storing credit card data are required to comply with the Payment Card Industry Data Security Standard (PCI DSS) by validating PCI DSS compliance. The PCI DSS is a common set of industry standards to educate businesses on the necessary steps to help ensure the safe handling of sensitive information. The standard was created to better align the separate card brand security programs into one, making it easier for merchants to comply with all card brands regulations. PCI DSS validation applies to ALL organizations or merchants that accept, transmit, or store any cardholder data regardless of size or number of transactions.

Validating compliance consists of completing a Self-Assessment Questionnaire (SAQ) specific to your card holder data environment. In addition to completing a SAQ, some merchants are also required to perform quarterly vulnerability scanning and annual penetration testing. Businesses who have already validated are asked to provide proof in the form of an Attestation of Compliance and passing Approved Scanning Vendor vulnerability scan (if applicable) for review.

**How long does it take to become compliant?**

The amount of time it takes for a company to validate compliance is dependent on the amount of time it takes to complete the Self-Assessment Questionnaire and remediate the threats the vulnerability scan and penetration testing discovers (if scanning and testing are applicable). Some businesses handle cardholder data in more complicated ways than others – this tends to increase the time involved to become compliant.

**What happens if my business is not compliant?**

It is important to maintain compliance because it demonstrates to customers, vendors and suppliers your dedication to cardholder privacy. The PCI Security Standards Council does not manage compliance programs and does not impose any consequences for non-compliance. The individual payment brands, however, have their own compliance initiatives, including financial and operational consequences to certain businesses that are not compliant. Although validating compliance does not guarantee a business will not suffer a data compromise, which in most cases is not only financially but also brand damaging, it greatly reduces the chances of this happening.

**What support is offered to merchants?**

We have a fully staffed Compliance Team ready to answer any questions pertaining to PCI DSS validation and how the requirement apply to your transaction processing method. In addition to the support we offer, our sponsored online validation program, SimplePCIDSS, offers access to a streamlined Self-Assessment Questionnaire (SAQ), in addition to access to quarterly vulnerability scanning performed by an Approved Scanning Vendor (ASV) and penetration testing tools.

**What are my businesses specific requirements for PCI DSS Compliance?**

The requirements for becoming PCI DSS compliant are dependent upon the merchant level that a company falls under. Merchants are divided into four different levels based on the number of VISA transactions they process throughout a year and the environment in which they operate. MasterCard also has merchant levels that dictate validation responsibilities.

**Does my business require vulnerability scanning to validate compliance?**

If you electronically store cardholder data or if your processing systems have any internet connectivity, a quarterly scan by a PCI SSC Approved Scanning Vendor (ASV) is required. A vulnerability scan is run on an environment (computer system, website domain or server) with the purpose of identifying security vulnerabilities that could potentially be exploited. In addition to indicating weaknesses, the scan report will also offer remediation steps to either eliminate those vulnerabilities or reduce them to an acceptable level or risk.

**How often are scans required?**

If you have equipment that requires a scan, a scan must be performed quarterly at minimum. Scans must be conducted by a PCI SSC Approved Scanning Vendor (ASV).

**Which equipment types do not require a scan?**

Stand alone dial-up terminals do not require a scan currently. Most other payment vehicles (software, POS systems, IP connected terminals, online shopping carts and certain payment gateway integrations) do require a scan.

**What is penetration testing?**

Penetration testing is an authorized ‘attack’ on a computer system or website with the intention of finding security weaknesses in its functionality and data. Penetration testing can help determine whether a system is vulnerable to attack, if the defenses in place are sufficient and which defenses (if any) were defeated in the penetration testing.

**What are the VISA merchant ‘levels’ as they relate to compliance validation and how are they determined?**

All merchants will fall into one of the four merchant levels based on Visa transaction volume over a 12-month period. Merchant levels as defined by Visa:

|  |  |
| --- | --- |
| **Merchant Level** | **Description** |
| **1** | Any merchant -- regardless of acceptance channel processing over 6M Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system |
| **2** | Any merchant -- regardless of acceptance channel processing 1M to 6M Visa transactions per year |
| **3** | Any merchant processing 20,000 to 1M Visa e-commerce transactions per year |
| **4** | Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants -- regardless of acceptance channel -- processing up to 1M Visa transactions per year |

**Where can I find the Payment Card Industry Data Security Standards (PCI DSS)?**

The Standard can be found on the PCI SSC's Website: <http://www.pcisecuritystandards.org>.