**What is PCI Compliance?**

The Payment Card Industry (PCI), which includes Visa, MasterCard, American Express and other leading card brands, requires service providers, banks and high-volume merchants to follow strict security guidelines, including:

* Building and maintaining a secure network.
* Protecting cardholder data.
* Maintaining a vulnerability management program.
* Implementing strong access control measures.
* Regularly monitoring and testing networks.
* Maintaining an information security policy.

In accordance with these guidelines and with a third-party security assessment, Pivotal Payments has been issued a certificate of PCI Compliance toward the requirements of the Payment Card Industry (PCI) Data Security Standards (DSS) validation methods.

**Importance of PCI Compliance for Your Business**

* Who does PCI Compliance apply to?
* PCI DSS requirements apply to all organizations or merchants who accept, transmit or store any cardholder data.
* What exactly is 'cardholder data'?
* Cardholder data is any and all information which can personally identify or be associated with the cardholder. Information such as name, address, account number etc. All personally identifiable information associated with the cardholder that is stored, processed, or transmitted is also considered cardholder data.
* What about debit card transactions?
* Within the scope of PCI DSS are all cards branded with one of the five card association/brand logos that participate in the PCI SSC - American Express, Discover, JCB, MasterCard, and Visa International. That includes debit cards and prepaid cards in addition to credit cards.
* What if I only accept credit cards over the phone, does PCI still apply to me?
* As mentioned above, any business which stores, processes or transmits card holder data must be PCI compliant.

**PCI Compliance SAQ**

* Where can I find the PCI Data Security Standards (PCI DSS)?
* You can find them on the PCI SSC's Website using the link below:
<https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml>
* Are there different PCI compliance 'levels'?
* Yes. There are four different merchant levels which are based on transaction volume over 12 months.

**See the table below for the different Merchant levels as defined by Visa:**

Merchant Levels 1,2,3,4;

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.

### *If my business has multiple locations do I need to validate PCI Compliance for each location?*

Unless each location processes under a different Tax ID then you are only required to validate once annually for all locations. You may also be required to submit quarterly passing network scans by a PCI SSC Approved Scanning Vendor (ASV), if applicable.

### *What are the penalties for noncompliance?*

Noncompliance can be very costly and although the payment brands fine the acquiring bank and not the merchant directly, penalties make their way downstream and could result in increased transaction fees or even termination of the banking relationship. An acquiring bank faces anywhere from $5,000 to $100,000 per month for PCI compliance violations.

### PCI Compliance: The Importance of Performing a Vulnerability Scan on a Regular Basis.

CLICK HERE>