

Credit Card Vaulting: Frequently Asked Questions

Q: What is PCI DSS?

A: The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that **ALL** companies that **process, store** or **transmit** credit card information maintain a secure environment. This applies to for-profit and non-profit organizations alike; essentially any merchant that has a Merchant ID (MID). The standard provides a framework for developing account data security processes - including preventing, detecting and reacting to security incidents.

Q: What is PCI SSC?

A: The Payment Card Industry Security Standards Council (PCI SSC) manages the ongoing evolution of the Payment Card Industry (PCI) security standards with a focus on improving payment account security throughout the transaction process. They are an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB). It is important to note, the payment brands and acquirers are responsible for enforcing compliance, not the PCI council. For more information about the PCI Security Standards Council, visit: www.pcisecuritystandards.org.

Q: What are the deadlines for complying with PCI DSS?

A: As of July 2010, any organization which accepts, transmits, or stores cardholder information is held to the new PCI DSS standards. The goal of the standards is to ensure card member safety. All entities that transmit, process or store payment card data must be compliant with PCI DSS.

Q: Do organizations using third-party processors have to be PCI compliant?

A: Yes. Merely using a third-party company does not exclude an organization from PCI compliance.

Q: What are the penalties for noncompliance?

A: Organizations that do not comply with PCI DSS may be subject to fines (up to \$10,000 per month), card replacement costs, costly forensic audits, damage to your reputation, loss of donor confidence, etc., should a breach event occur. For a little upfront effort and cost to comply with PCI, you greatly help reduce your risk from facing these costly consequences.

Q: Where can I find more information about PCI compliance?

A: A full version of the PCI DSS can be found on the Security Standards Council's website at: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml. For more information about PCI compliance in general, visit: www.pcicomplianceguide.org.