PCI FAQs

PCI FAQs

Fall 2014

PCI FAQS

What is PCI DSS and why was it created? The Payment Card Industry Data Security Standards (PCI DSS) is a set of requirements and best practices for enhancing payment account data security within business environments. These standards were developed by the PCI Security Standards Council, which was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa International to facilitate industry-wide adoption of consistent data security measures on a global basis.

Why does my business need to be PCI Compliant? By being PCI Compliant you help protect your business by reducing the risk of a costly breach of your customers' payment card data. In addition, the payment card brands (American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa International) mandate that all businesses processing payment cards must validate they are compliant with PCI DSS.

Once my business becomes PCI-DSS compliant, does that prevent a security breach from happening? No. These actions prescribed by PCI-DSS help prevent security breaches and loss of cardholder data but do not provide a guarantee to your business. If and when you change the manner in which you store, process or transmit cardholder data, you may increase the vulnerability of your business. Also, similar to the regularly required updates to anti-virus and firewall software, data security is also continually subject to new threats. We encourage you to stay up to date on all data security requirements.

Who should I contact for support in becoming PCI-DSS compliant? Our helpful online tool, the PCI Compliance Manager, will help you evaluate the status of your account, to assist with any necessary remediation efforts and to certify your account's PCI compliance. Please contact us for additional program details regarding the PCI Compliance Manager.

Do I have to use Elavon's PCI Compliance Manager to become compliant? No. There are many approved vendors. You are free to choose to certify with any vendor you like. A list of approved vendors is available on the payment card network website, www.pcisecuritystandards.org. But you will need to provide the validation documentation received through that vendor to us by uploading it into the PCI Compliance Manager tool.

What happens to my business if I am not PCI Compliant? If you do not comply with the security requirements contained within PCI-DSS as mandated by the payment card networks, you put your organization at risk of a payment card compromise. In the event that your business is compromised, you may be subject to additional fines, fees, and assessments by the card brands. You will also be liable for the cost of the required forensic investigations, fraudulent purchases, and the cost of re-issuing cards. You may also lose your credit card acceptance privileges.

We may impose additional fees for each month that your account has not been validated as PCI compliant or in any given month your account is deemed non-compliant. You must maintain your compliant status once it is obtained in order to prevent this fee in the future.

What am I required to do to become PCI Compliant? The minimum requirement for a level 4 business is to complete a PCI-DSS Self-Assessment Questionnaire (SAQ) on an annual basis and achieve a passing status. If you electronically store cardholder information or if your processing systems have any internet connectivity, a quarterly network vulnerability scan by an approved scanning vendor is also required.

Which PCI Self-Assessment Questionnaire (SAQ) do I need to complete? The PCI Self-Assessment Questionnaire is a list of questions used to assess your compliance with the requirements of the PCI-DSS. In February of 2008, the PCI Security Standards Council released four versions of the questionnaire to account for different merchant environments.

1. SAQ A: Addresses requirements applicable to businesses that have outsourced all cardholder data storage, processing and transmission.
2. SAQ A-EP: Addresses requirements applicable to ecommerce businesses that capture the cardholder data as part of the transaction process. This also requires vulnerability scanning and penetration testing on the cardholder data environment.
3. SAQ B: Created to address requirements pertinent to businesses that process cardholder data via imprint machines or standalone dial-up terminals only.
4. SAQ B-IP: Created to address requirements related to businesses that process cardholder data via a POS terminal using an Ethernet (internet) connection.
5. SAQ C: Constructed to focus on requirements applicable to businesses whose payment applications systems are connected to the Internet.
6. SAQ C-VT: Developed for those businesses who process using a virtual terminal (access POS via a hosted user interface).
7. SAQ D: Designed to address requirements relevant to all businesses defined by a payment brand as storing cardholder data electronically or those businesses who do not fall under the types addressed by SAQ A, B or C.

What if I fail PCI Validation? If you fail PCI Validation that means that the quarterly vulnerability scan discovered areas of vulnerability in your network of high severity or business practices answers you provided on the SAQ is not incompliance with the PCI DSS. The PCI Compliance Manager will help guide you to remediate a failed scan and work toward achieving compliance. If failing a vulnerability scan, first, you'll want to login to your PCI Compliance Manager account to review the scan results. The report will provide a description of the identified issues and resources to begin fixing the problems. You'll need to address each of the problems and then schedule a directed scan to ensure your remediation of the problem meets the PCI-DSS requirements.

What if I am required to upgrade my equipment or software to become compliant? As part of becoming PCI compliant you may be required to upgrade your equipment and/or software to a PCI-DSS certified version. You must contact your equipment and/or software vendor to discuss what options may be available and the costs associated with those options, if any. The cost associated with any equipment and/or software upgrade will not be covered by us.

How long is the PCI compliance certification valid? The length a PCI compliance certificate is valid depends on whether your business requires a questionnaire or scan. If your business only requires the annual questionnaire, PCI Certification is valid for one year. If your business requires quarterly scans, PCI Certification is valid for three months at which time your next quarterly scan will be due. If you change the manner in which you store, process or transmit cardholder data, you may increase the vulnerability of your business and must revalidate compliance with your new environment immediately.

What if I have already performed my PCI Compliance self-assessment questionnaire (and applicable quarterly scans)? If you have already validated PCI Compliance for your business via another PCI Program other than ours, you must supply proof of validation by choosing your processing method - either IP or Non-IP solutions - and following the instructions until you are prompted to supply your proof of PCI-DSS compliance validation to us.