

Compliance Assistance Program

Frequently Asked Questions of Level-4 Merchants

What is PCI DSS?

The Payment Card Industry Data Security Standards (PCI-DSS) is a set of requirements for enhancing payment account data security. 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.

I have never heard of PCI Compliance before, is this new?

No. Merchants have been advised to take the PCI Self-Assessment Questionnaire (SAQ) to identify potential security risks in order to achieve PCI compliance for the past several years. The framework of the PCI data security standards is not new and has been required in different forms for some time now and continues to evolve. You may be more familiar with the payment brands' programs that promote the implementation of the PCI-DSS:

- MasterCard: Site Data Protection (SDP) program - www.mastercard.com/sdp
- VISA: Cardholder Information Security Program (CISP) – www.visa.com/cisp
- Discover Network: Discover Information Security & Compliance (DISC) – www.discovernetwork.com/fraudsecurity/disc.html
- American Express: Data Security Operating Policy – www.americanexpress.com/datasecurity

What am I required to do to become PCI Compliant as a level 4 merchant?

The minimum requirement for a level 4 merchant is to complete a PCI DSS Self-Assessment Questionnaire (SAQ) on an annual basis and achieve a passing score. If you electronically store cardholder information or if your processing systems have any internet connectivity, a quarterly scan by an approved scanning vendor is also required.

How long will obtaining PCI Compliance take?

The time it takes an individual business to become PCI compliant can vary based on how the business processes, stores, or transmits cardholder data.

Self Assessment Questionnaire = 1 to 8 hours

IP Scans = 4 to 6 hours*

*Depending on the complexity of your system this process may take additional time.

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 contact DeviceLogix to re-assess your compliance posture.

Am I required to certify for PCI Compliance?

Yes, the payment brands require all acquirers to report on the PCI compliance of their merchants. If you do not complete the Self-Assessment Questionnaire you may overlook certain data security practices that minimize your risk of a security breach. In the event that your business is compromised, you may be subject to fines of up to \$500,000 per payment brand. These fines do not include the expenses or cost of fraudulent transactions resulting from the breach. In addition to avoiding potential fines, PCI compliance may give your customers confidence that their credit card information is protected at your business.

I only process a few hundred dollars a month. Does my merchant account still need to be PCI Compliant?

Yes, all merchants, whether small or large, need to be PCI compliant. The payment brands have collectively adopted PCI-DSS as the requirement for organizations that process, store or transmit payment cardholder data. Inherent in having a merchant account is the ability to handle cardholder data.

I'm already using a "PCI compliant" terminal/gateway. Why do I have to have my account certified for PCI compliance?

The PCI Security Standards Council has various requirement programs. The Payment Application Data Security Standards (PA-DSS) is a set of requirements to help software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with the PCI-DSS.

Use of a terminal/gateway that runs PA-DSS certified software is one of many components that are evaluated in the assessment of an account's PCI-DSS compliance.

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 DeviceLogix.

Can I choose not to certify for PCI Compliance?

No, the payment brands require all acquirers to report on the PCI compliance of their merchants. If you choose not to complete the self-assessment questionnaire you may overlook certain data security practices that minimize your risk of a security breach. In the event that your business is compromised, you may be subject to fines of up to \$500,000 per payment brand. These fines would be in addition to the expenses and fraudulent transactions resulting from the breach.

In light of the importance that data security has to the payment processing industry and consumers at large, your merchant services provider may also begin imposing a fee for each month that your account has not been validated as PCI compliant or in any given month your account is deemed non-compliant.

Once my business becomes PCI DSS compliant, does that prevent a security breach from happening?

These actions help prevent security breaches 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.

DEVICELOGIX[™]
The Better Business Builder

17774 Cypress Rosehill Road

Suite 1600

Cypress, TX 77429

281-255-4440

1-800-69-LOGIX