

PCI Compliance Validation Service Program

Frequently Asked Questions

What is PCI DSS?

The Payment Card Industry (PCI) Data Security Standard (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, Inc. to facilitate industry-wide adoption of consistent data security measures on a global basis. The standard aims to increase awareness and promote best practices in the handling of sensitive information as a means to minimizing identity theft and fraudulent transactions.

Is PCI DSS new?

No. The framework of the PCI data security standards has existed in different forms for some time now and continues to evolve. You may be more familiar with the payment brands' programs that promote the adoption of the PCI DSS

- MasterCard: Site Data Protection (SDP) program
 - Mastercard.com/sdp
- Visa: Cardholder Information Security Program (CISP)
 - Visa.com/cisp
- Discover Network: Discover Information Security & Compliance (DISC)
 - Discovernetwork.com/fraudsecurity/disc.html
- American Express: Data Security Operating Policy
 - AmericanExpress.com/datasecurity

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, are required to be PCI compliant. The payment brands have collectively mandated PCI DSS compliance for any and all organizations that process, store or transmit payment cardholder data. Inherent in having a merchant account is the ability to handle cardholder data.

I already use a "PCI compliant" terminal/gateway. Doesn't that mean I am PCI compliant?

No. Use of a PCI compliant payment application is one aspect of the many PCI DSS requirements, which cover handling of sensitive data. Currently, the PCI DSS lists twelve requirements. These requirements are organized around the following principles:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

Can I choose not to certify for PCI compliance?

If you choose not to complete the self-assessment questionnaire (and applicable network scans) 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 substantial fines 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, we, as your service 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. Failure to validate compliance may result in the termination of your merchant account.

What do I need to do to validate my PCI DSS compliance?

We have established a relationship with SecurityMetrics, Inc., a leading provider of PCI audit and scan services. SecurityMetrics' service includes: assistance in determining which version of the Self-Assessment Questionnaire is appropriate for your business; administration of any applicable network scans; guidance on any necessary remediation efforts; and certification and validation of your account's compliance. These SecurityMetrics services are available to you as part of our *PCI Compliance Assistance Service Program*. You can take advantage of this opportunity by enrolling with SecurityMetrics via their Web site securitymetrics.com or by calling (800) 557-4684.

How long is the PCI compliance certification valid?

The PCI compliance certificate is valid for one year from the date the certificate is issued. To maintain your compliance, you are required to complete the PCI DSS self-assessment questionnaire annually and conduct any applicable network scan on a quarterly basis.

Do I have to use SecurityMetrics?

No. There are more than 130 qualified security assessors and approved scanning vendors. You are free to choose to certify with any vendor you like. However, if you choose to certify with another vendor you will be responsible for paying the full cost of the PCI Compliance analysis to that vendor. A list of approved vendors is available on the card association web sites or at pcisecuritystandards.org.

What if I have already been certified or choose to certify through another Qualified Security Assessor (QSA)/Approved Scanning Vendor (ASV)?

If you have already been PCI DSS certified or if you choose to use another QSA/ASV, please submit your certification documentation to us via e-mail at pci.1@firstdata.com or fax to (402) 916-8240.