

Payment Card Industry Data Security Standard (PCI DSS) Frequently Asked Questions

1. **What is PCI DSS?**

The Payment Card Industry Data Security Standard (PCI DSS) was created by the five major credit card companies as a guideline to help business owners implement the necessary hardware, software and other procedures to guard sensitive credit card and personal information. PCI DSS is a set of requirements for enhancing payment account data security. The five major credit card companies that developed the PCI Security Standards Council are American Express®, Discover® Financial Services, JCB International, MasterCard® and Visa®.

2. **What does PCI compliance mean?**

PCI compliance means that your business is exhibiting best practices to prevent cardholder information or data security breaches. While PCI compliance is not a guarantee of security, it is an important step in prevention.

3. **I have never heard of PCI compliance before. Is this new?**

No. Business owners began taking the PCI Self-Assessment Questionnaire (SAQ) to identify potential security risks to achieve PCI compliance starting in 2005. You may be more familiar with the payment brands' programs that promote the implementation of the PCI DSS:

- MasterCard: [Site Data Protection \(SDP\) Program](#)
 - Visa: [Cardholder Information Security Program \(CISP\)](#)
 - Discover Network: [Discover Information Security & Compliance \(DISC\)](#)
 - American Express: [Data Security Operating Policy](#)
-

4. **What am I required to do to become PCI compliant?**

The minimum requirement is to complete a Payment Card Industry Data Security Standard 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.

Merchant Services has created a complete reference guide on becoming PCI compliant. Our guide breaks down compliance into five easy steps: [Enroll](#), [Comply](#), [Validate](#), [Certify](#) and [Renew](#).

5. **How long will obtaining PCI compliance take?**

The time it takes a business to become PCI compliant can vary based on how your business processes, stores or transmits cardholder data. It takes about five to 10 minutes to enroll in the program and 15 minutes to complete the self-assessment questionnaire. In less than 30 minutes, you could be PCI compliant.

6. **How long is the PCI compliance certification valid?**

The length a PCI compliance certificate is valid depends on whether your business requires a questionnaire and, where applicable, a scan. If your business requires only the questionnaire, the PCI certification is valid for one year. If your business also requires quarterly scans, the 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 will need to contact [SecurityMetrics](#), our PCI compliance partner, or another third-party vendor for recertification.

7. **Am I required to certify for PCI compliance?**

Yes, all acquirers are required to report on the PCI compliance of their businesses. If you do not complete the self-assessment questionnaire, you may overlook data security practices that minimize your risk of a security breach. In the event your business is compromised, you may be subject to fines of up to \$500,000 per Association. These fines do not include the expenses or costs 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.

Your Merchant Processor may also impose a fee for each month your account has not been validated as PCI compliant or in any given month your account is deemed noncompliant.

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

Yes. The Associations have collectively adopted the PCI Data Security Standard as the requirement for businesses that process, store or transmit payment cardholder data, no matter how many cards are processed. Inherent in having a merchant account is the ability to handle cardholder data.

9. **I'm a seasonal business that processes only three months out of the year. Does my merchant account still need to be PCI compliant?**

Yes. The Associations have collectively adopted PCI Data Security Standard as the requirement for all businesses that contact cardholder data, even if seasonal. Inherent in having a merchant account is the ability to handle cardholder data.

10. **My business has multiple locations. Is each location required to certify?**

If your business locations process under the same Tax ID number, you are required to certify only once for all locations. However, if your business locations have different Tax ID numbers and if you disclose to [SecurityMetrics](#) how your businesses are storing, processing or transmitting credit card data, you have to certify only once. To ensure you complete only the necessary certifications, verify upon enrollment with SecurityMetrics, our PCI partner, or the vendor you are using that each location is linked together.

11. **I'm already using a PCI-compliant terminal/gateway. Why does my account need to be certified for PCI compliance?**

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

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.

12. **Whom should I contact for support in becoming PCI compliant?**

Merchant Services has partnered with [SecurityMetrics](#) to help you evaluate the status of your account, to assist with any necessary remediation efforts and to certify your account's PCI compliance. In addition to [signing up online](#), you can also call SecurityMetrics at 800-557-4684. You'll need to identify yourself as a merchant of First Data Merchant Services.

13. **What are the hours of operation for SecurityMetrics?**

Enrollment with [SecurityMetrics](#) is available Monday–Friday, 4:00 am–10:00 pm ET. SecurityMetrics technical support is available 24/7 to assist with data security concerns. If you choose to use a third-party vendor, you'll need to inquire as to its hours of operation.

14. **Do I have to use SecurityMetrics?**

No. There are more than 100 approved PCI vendors. You are free to certify with any vendor you like. The benefits of using [SecurityMetrics](#) are that you receive a low-cost or no-cost PCI assessment and your certification is sent directly to us from the vendor.

If you choose to use another vendor, you will need to pay full cost of the PCI assessment. In addition, you'll need to forward a copy of the PCI compliance analysis to us. A list of approved vendors is available at [PCI Security Standards](#). If you choose to use a third-party vendor, [instructions](#) to send your compliance certification to us is available.

15. **How do I identify myself with SecurityMetrics that I am a First Data Merchant Services customer?**

Registering Online

On the **Purchase Information** screen, select **Acquiring Bank** from the drop-down menu and then select **First Data Merchant Services**. You will be prompted to enter the last six digits of your merchant account number (you can get your merchant account number from your Merchant Services statement) and your zip code.

Merchant Services has negotiated preferred rates with [SecurityMetrics](#). By identifying yourself as a First Data Merchant Services customer, you will receive the lowest cost option for your PCI assessment and your certification is sent directly to us from PCI.

Registering by Phone

Call 800-557-4684 and tell the representative you are with First Data Merchant Services. The representative will ask for your phone number to locate your account and will confirm the last six digits of your merchant account number as it appears on your Merchant Services statement.

16. **Is there a charge for SecurityMetrics' services?**

Merchant Services has negotiated preferred rates with [SecurityMetrics](#). The potential charge will vary depending on the level of service needed for your account. The cost associated with the questionnaire and, where applicable, a quarterly scan will be provided during enrollment with SecurityMetrics.

17. **Will there be an additional cost for each of my business locations?**

To ensure you obtain the preferred rates when you enroll, you must verify with [SecurityMetrics](#) that each location is linked together at the time of enrollment. If you use a third-party vendor, you will need to inquire with that company for pricing at multiple locations.

18. **Is there an additional cost for quarterly scans?**

If your business requires a quarterly scan, any associated cost will be built into the price quoted when you enroll with [SecurityMetrics](#). If additional IP addresses are added to your business between scans, there may be additional costs. Contact SecurityMetrics or your third-party vendor to discuss the costs.

19. **Will I be provided with anything that I can display to my customers showing that I am a PCI-compliant merchant?**

Yes. After you've completed your certification, there is a certificate of compliance available through your [SecurityMetrics](#) account. If you would like a logo of certification to display on your Web site, you'll need to request one from SecurityMetrics. If you have a third-party vendor, you will need to inquire with that company as to what documentation it will provide to you and in what time frame.

20. **What if I have already performed my PCI compliance self-assessment questionnaire (and applicable quarterly scans)?**

If you used SecurityMetrics to become PCI Data Security Standard certified, [SecurityMetrics](#) will validate your responses with Merchant Services directly. You need to ensure your SecurityMetrics account has been associated with First Data Merchant Services.

If you used a third-party vendor, you will need to submit all of your certification documentation to us so that we know that your account is currently PCI compliant. Instructions on how to send your compliance certification to us are [available](#).

21. **Will I need to upgrade my equipment or software to become PCI compliant?**

As part of becoming PCI compliant, you may be required to upgrade your equipment and/or software to a PCI Data Security Standard certified version. You will need to contact your equipment and/or software vendor to discuss what options may be available and the costs associated with those options. The costs associated with any equipment and/or software upgrade will not be covered by [SecurityMetrics](#) or Merchant Services.

22. **Can I choose not to become PCI compliant?**

No. The Associations 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 could increase 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 Association. These fines would be in addition to the expenses and fraudulent transactions resulting from the breach.

Your Merchant Processor 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 noncompliant.

23. **How do I prevent or eliminate a non-receipt of PCI data validation fee?**

You can prevent or eliminate this charge by validating your PCI Data Security Standard compliance with [SecurityMetrics](#) or an approved third-party vendor on or before the 25th day of the month your certification or renewal is due.* If you choose to use SecurityMetrics, your certification will be validated with Merchant Services directly.

If you choose to use a third-party vendor, instructions to send your compliance certification to us is [available](#). Your certification must be received by Merchant Services on or before the 25th to prevent a non-receipt of PCI validation fee.

*If the 25th falls on a weekend, documentation needs to be provided Friday before the weekend.

24. **If I change the way in which my business stores, processes or transmits cardholder data, am I required to recertify and will there be extra charges?**

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 [SecurityMetrics](#) or your third-party vendor for recertification.

Based on how you change your processing, there may be an additional charge. To determine what, if any, additional charge may be incurred, contact SecurityMetrics or your third-party vendor.

25. **After my business becomes PCI Data Security Standard compliant, does that prevent a security breach from happening?**

These actions help prevent security breaches, but do not provide a guarantee to your business. But if a breach occurs, it will reduce or eliminate fines from the card brands. Also, it's important to install regular anti-virus and firewall software updates. Data security is continually subject to new threats, and these updates will help reduce those threats. We encourage you to stay up-to-date on data security requirements.

26. **I'm a new business owner. Am I eligible for the SecurityMetrics preferred rate?**

Yes. [SecurityMetrics](#) offers the Merchant Services preferred rate to any new business owner.

It may take up to six weeks following the boarding of your account with Merchant Services for SecurityMetrics to recognize your account.

27. **What is a Qualified Security Assessor?**

A Qualified Security Assessor (QSA) is an organization that has been qualified by the PCI Security Standards Council. Qualified Security Assessors are employees of these organizations who have been certified by the Council to validate a business's adherence to the PCI Data Security Standard.

28. **What is an Approved Scanning Vendor?**

Approved Scanning Vendors (ASVs) are organizations that validate adherence to certain PCI Data Security Standard requirements by performing vulnerability scans of Internet-facing environments of businesses and service providers.