

PCI | Frequently Asked Questions

Did you know?

- Eighty percent of payment card data compromises occur at brick-and-mortar merchants, compared to 20 percent at e-commerce merchants.
- Ninety-six percent of payment card data compromises occur at brick-and-mortar locations due to non-PCI compliant payment applications.
- Half of payment card data compromises are blamed on third-party negligence.

What is the PCI DSS?

The PCI DSS is a set of comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council (American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International), to help facilitate the global adoption of consistent data security measures. The PCI DSS includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures intended to proactively protect customer account data.

Are all Businesses and Service Providers required to comply with the PCI DSS?

Yes. All entities (businesses or service providers) that store, process, or transmit cardholder data must comply with the PCI DSS. The requirements apply to all acceptance channels including retail (brick-and-mortar), mail/telephone order (MOTO) and e-commerce. Validation requirements vary depending on Service Provider or Merchant level.

Is this a onetime requirement?

No. Validation actions vary depending on Service Provider or Merchant level. However, the credit card associations require all businesses accepting card-based payments to comply with PCI DSS at all times. There are two main components of validation:

1. Completing the PCI Self-Assessment Compliance Questionnaire annually
2. Undergoing Vulnerability Scans performed by an Approved Scanning Vendor quarterly

What if my business does not go through this compliance procedure?

If you do not comply with the security requirements of the card associations, you put your organization at risk of payment card compromise. Your acquirer may pass fines levied by the card associations for non-compliance on to you, or you may even lose the ability to process credit cards.

Do I get anything to prove I am compliant, if so, will it be automatically sent to Visa or MasterCard?

Once you have successfully completed the compliance program, you will receive a Certificate of Compliance. Any reporting to your acquirer will be facilitated by your consultant. It is the acquirer's responsibility to report statuses to the Card Associations.

Can our internal staff validate our compliance?

No. The card associations require that you use an Approved Scanning Vendor to perform the quarterly vulnerability scans. However, your internal staff can complete the Annual PCI Self-Assessment questionnaire.

We don't have time for this. How long will this take?

The length of the process varies. Once non-compliance issues have been identified, the length of time it takes an organization to implement solutions to resolve the issues will affect the length of the PCI DSS compliance process. The length of time also varies depending on the resolution and the complexity of the environment.

What are the requirements for PCI DSS?

There are twelve requirements that fall into six categories:

1. **Build and Maintain a Secure Network:** Install and maintain a firewall, and use unique, high-security passwords, with special care to replace default passwords. Do not use vendor-supplied defaults for system passwords and other security parameters
2. **Protect Cardholder Data:** Whenever possible, do not store cardholder data. You must also encrypt any data passed across public networks, including your shopping cart and web-hosting providers.
3. **Maintain a Vulnerability Management Program:** Use anti-virus and keep it up date. Develop and maintain secure operating systems and payment applications. Ensure the applications your use are compliant (see www.visa.com/pabp).
4. **Implement Strong Access Control Measures:** Access – both electronic and physical access – to cardholder data should be on a “need-to-know” basis. Ensure those people with access have a unique ID and password. Do not share logon information.
5. **Regularly Monitor and Test Networks:** Track and monitor all access to networks and cardholder data. Ensure you have a regular testing schedule for security systems and processes: firewalls, patches and anti-virus.
6. **Maintain an Information Security Policy:** It's critical that your organization has a resource for how data security is handled at your business. Ensure you have a policy and that it's disseminated and updated regularly.

How is “cardholder data” defined?

Cardholder data is the full magnetic stripe or the Primary Account Number plus any of the following:

- Cardholder Name
- Expiration Date
- Service Code

The PCI DSS applies to any businesses that store, process, transmit or have access to cardholder data.

What’s my next step?

Call your partner at the WAC Consulting Group to get started on the analysis and compliance process.

Call 866.400.0922 or email Mary Clark at mary.clark@waccg.com

More Resources at

www.waccg.com/business-software-solutions/pci-resource-center.php