PCI DSS FAQs

What is the Payment Card Industry (PCI) Data Security Standard (DSS)?

The PCI Data Security Standard represents a common set of industry tools and measurements to help ensure the safe handling of sensitive information. It is comprised of 12 general requirements designed to: build and maintain a secure network; protect cardholder data; ensure the maintenance of vulnerability management programs; implement strong access control measures; regularly monitor and test networks; and ensure the maintenance of information security policies.

Why Comply with PCI Security Standards?

Why should you, as a merchant, comply with the PCI Security Standards? At first glance, especially if you are a smaller organization, it may seem like a lot of effort, and confusing to boot. But not only is compliance becoming increasingly important, it may not be the headache you expected.

Compliance with data security standards can bring major benefits to businesses of all sizes, while failure to comply can have serious and long-term negative consequences. Here are some reasons why.

- Compliance with the PCI DSS means that your systems are secure, and customers can trust you with their sensitive payment card information:
  - Trust means your customers have confidence in doing business with you
  - Confident customers are more likely to be repeat customers, and to recommend you to others

- Compliance improves your reputation with acquirers and payment brands -- the partners you need in order to do business

- Compliance is an ongoing process, not a one-time event. It helps prevent security breaches and theft of payment card data, not just today, but in the future:
  - As data compromise becomes ever more sophisticated, it becomes ever more difficult for an individual merchant to stay ahead of the threats
  - The PCI Security Standards Council is constantly working to monitor threats and improve the industry’s means of dealing with them, through enhancements to PCI Security Standards and by the training of security professionals
  - When you stay compliant, you are part of the solution – a united, global response to fighting payment card data compromise

- Compliance has indirect benefits as well:
  - Through your efforts to comply with PCI Security Standards, you’ll likely be better prepared to comply with other regulations as they come along, such as HIPAA, SOX, etc.
  - You’ll have a basis for a corporate security strategy
  - You will likely identify ways to improve the efficiency of your IT infrastructure

- But if you are **not** compliant, it could be disastrous:
    - Compromised data negatively affects consumers, merchants, and financial institutions
    - Just one incident can severely damage your reputation and your ability to conduct business effectively, far into the future
    - Account data breaches can lead to catastrophic loss of sales, relationships and standing in your community, and depressed share price if yours is a public company
    - Possible negative consequences also include:
        - Lawsuits
        - Insurance claims
        - Cancelled accounts
        - Payment card issuer fines
        - Government fines

You've worked hard to build your business – make sure you secure your success by securing your customers' payment card data. Your customers depend on you to keep their information safe – repay their trust with compliance to the PCI Security Standards.

What are the consequences to my business if I do not comply with the PCI DSS?

The PCI Security Standards Council encourages all businesses that store payment account data to comply with the PCI DSS to help lower the brand and financial risks associated with account payment data compromises. The PCI Security Standards Council does not manage compliance programs and does not impose any consequences for non-compliance. Individual payment brands, however, may have their own compliance initiatives, including financial or operational consequences to certain businesses that are not compliant.

How do you comply with the PCI DSS?

It's a matter of following the 12 requirements in the standard, working with your acquiring bank and using the tools offered through the Council. Remember that PCI DSS compliance is an ongoing process, not a one-time event. You'll need to continuously assess your operations, fix any vulnerabilities that are identified, and make the required reports to the acquiring bank and card brands you do business with.

What does PCI DSS compliance mean?

In security terms, it means that your business adheres to the PCI DSS requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. In operational terms, it means that you are playing your role to make sure your customers' payment card data is being kept safe throughout every transaction, and that they – and you – can have confidence that they're protected against the pain and cost of data breaches.