**Target Keyword:** What is PCI Compliance and Why Does It Matter for Your Business?
**Word Count:** 750
**Page Title:** What is PCI Compliance and Why Does It Matter for Your Business?

With identity theft on the rise, PCI compliance standards were set up in 2006 as a means to strengthen security for customers who engage in credit card transactions. PCI, also known as Payment Card Industry Data Security Standard or PCI DSS, represents the series of requirements that businesses must adhere to when they store, process, or transmit data from credit cards in a secure environment.

## The history

In 2006, the PCI Security Standards Council was established, and is comprised of major credit card companies American Express, Discover, MasterCard, Visa, and the Japanese Credit Bureau, or JCB.

With the establishment of the PCI Security Standards Council, a structure and protocols were put in place to evaluate the PCI security standard on an ongoing basis, and to implement improvements to security as much as possible as they become available. This across-the-board standard replaced previously uneven compliance standards in the industry.

What this means in regard to what is PCI compliance and why does it matter for your business is that there are now a strict set of requirements that are continually enforced and monitored by the credit card companies who make up the PCI Council; those requirements must be met by all business owners, including small business owners. In short, if you are a business that processes, stores, and/or transmits credit card information, you must comply with PCI standards. If you accept credit cards, you must:

- Maintain your network securely
- Protect cardholders' data and personal information
- Maintain a program that addresses vulnerability management
- Utilize strong measures that address access control
- Test and monitor networks regularly
- Develop, implement, and maintain a security policy for information

While the above generalizations comprise a sort of "cheat sheet" to monitor that you are in fact meeting PCI standards in regard to what is PCI compliance and why does it matter for your business, a more in-depth list of requirements is explained below.

## The 12-point test you must pass to ensure that you are meeting PCI security standards

The PCI Security Standards Council has developed a 12-point test that covers different payment channels, transaction volumes, and the level of exposure inherent in particular companies. All companies must comply with the 12-points as enumerated in the test to ensure that they are compliant with PCI security standards. To be fully compliant in regard to what is PCI compliance and why does it matter for your business, you must:

- Use and update antivirus software on a regular basis
- Fully encrypt transmission of data from cardholders, especially when you're on public or open networks
- Protect data cardholders store with you
- Implement and maintain a secure firewall configuration so that cardholders' data is fully protected at all times
- Avoid use of vendor-supplied security parameters, such as passwords and other devices
- Give each person who has computer access for your business a unique ID
- Limit employees' access to cardholders' information on a need-to-know basis
- Limit or deny physical access to cardholder data within your business to in place as a matter of policy (and again only on a need-to-know basis)
- Monitor and track network resource access and cardholder data access continuously
- Implement regular testing of security processes and systems
- Develop and maintain an information security policy for your business
- Make sure systems and applications are secure at all times, developing systems and processes to do so if necessary

It's important to note that to be truly compliant with PCI regulations, you must meet ALL 12 requirements, at all times. If you fail just one of these points, or are "just" 99% compliant, you fail PCI standards. While this may be problematic for smaller companies with limited resources, such strict rules ensure that your customers' data is protected – and that their risk of identity theft when they use their credit cards online or via phone is small. You must also ensure that credit card data given over the phone is protected and PCI compliant.

Penalties for noncompliance can be steep in regard to what is PCI compliance and why does it matter for your business; the credit card companies of the PCI Security Standards Council don't fine business owners directly for noncompliance, but they do fine the acquiring banks anywhere from $5000 to $100,000 per month for any violations. Banks, of course, will likely pass these fines onto mergers, and either terminate your relationship altogether or boost your transaction fees if you are found continually not compliant.  Make sure you are fully versed in what your merchant account agreement contains; it should tell you what your exposure is and what you must do to mitigate it.