Protect Your Customers' Data and Your Business

DataGenesis

Cardholder Security and Payment Card Industry (PCI) Compliance —and How We Can Help

What Is PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) was created by the 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. The object of becoming compliant with PCI security standards is to help protect sensitive cardholder data from data thieves.

One of the most significant PCI DSS requirements is that a merchant may not store magnetic-stripe data after an authorization is obtained on a credit card.

What Does PCI Compliance Mean

PCI compliance means that your business is exhibiting best practices to prevent cardholder information or data breaches

How To Become PCI Compliant

After receiving your user name and password visit www.pcirapidcomply.com. The step-by-step guided application will direct you to the appropriate self-assessment questionnaire (SAQ) for your business. The average amount of time to complete the SAQ and become compliant:
Questionnaire A or B = 15 – 30 minutes
Questionnaire C or D = 45 minutes or more
IP Scans = 15 minutes *depending on the complexity of your system.

Have a Question?

With the built-in help, guides and security expertise is available. PCI questions can be answered online, via chat, email and by phone. Call 1.855.532.4891 for assistance.

Contact Data Genesis 1.855.295.8500

What You Need to Know About PCI Compliance

Q. Why is PCI compliance required?
A. In 2005, the payment card networks established a common set of industry requirements designed to help with the safe handling of sensitive payment card account information. These requirements are known as the Payment Card Industry (PCI) Data Security Standard (DSS). These PCI security requirements have been phased in over time and now apply to all merchants that accept Visa, MasterCard and other payment cards.

Q. Is my business required to use Rapid Comply to become PCI compliant?
A. No, there are other options available to you. Please visit any of the following Web sites for additional information.
PCI Standards Council—PCISecurityStandards.org
Visa—usa.visa.com/merchants/risk_management/cisp.html
MasterCard—mastercard.com/us/sdp

If you choose to use another third-party vendor for PCI DSS compliance services, you will need to contract with and pay that vendor directly. In addition to your alternate vendor's charges, you will still need to pay the Compliance Services Fee charged to you by your Merchant Services provider. You will also need to ensure your PCI DSS compliant status is reported to Data Genesis.

Q. I already use a "PCI Compliant" terminal or gateway. Does that mean I am already PCI complaint?
A. 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 principals:

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

Q. What if my business fails to become PCI compliant?
A. The Card Associations are very serious about data security. You will be charged a monthly non-receipt of PCI validation fee for each month of non-compliance. Security breaches have affected merchants of all sizes. If your business is compromised, the Association fines can range up to $500,000 per Association. These fines are in addition to other liabilities your business may face in connection with a security breach.

For more information, please contact Data Genesis 1.855.295.8500 or email info@datagenesis.com.