

# First Data® PCI Rapid Comply<sup>SM</sup> Solution

Our PCI Rapid Comply<sup>SM</sup> solution is an easy-to-use online tool that can help you achieve and maintain PCI DSS compliance more quickly and easily.

## Go Beyond: First Data® PCI Rapid Comply Solution

If you are not aware, the PCI DSS Council (Payment Card Industry Data Security Standard) mandates security requirements for businesses of all sizes. The goal is to help protect cardholder and other sensitive data from data thieves.

As a merchant, you may have found the PCI DSS compliance process to be an overwhelming but necessary task to deal with. It can be daunting to understand PCI DSS compliance requirements and fill out the annual PCI SAQ (self-assessment questionnaire). For example, how would you answer a question like, "Are default SNMP community strings on wireless devices changed?"

## First Data Advantages

With our PCI Rapid Comply solution, you don't have to be a security expert to become and remain PCI DSS compliant. Our online solution is designed by PCI security experts specifically for small to mid-size merchants. And it turns PCI DSS jargon into clear language, with expert help to guide you through the PCI SAQ.

### Complete the required annual PCI SAQ with ease

Our step-by-step application will direct you to the PCI SAQ that is appropriate for your business (A, B, C, C-vt or D). You can complete the SAQ with guided support, ensuring each question is answered accurately.

### Answer fewer questions – in some cases, 85% fewer questions

With "pre-SAQ" questions, we can pre-populate the appropriate SAQ answers – which are often the most difficult – minimizing the number of questions you have to deal with and speeding up the SAQ completion process.<sup>1</sup>

### 24 x 7 availability to finish on time and on your schedule, not ours

Because our PCI Rapid Comply solution is an online tool, you have access to the SAQ and scanning tool if required anytime, letting you achieve PCI compliance on your schedule.

### Simple dashboard lets you know where you are in the process

With an interactive, real-time dashboard, you'll know where you are in the PCI DSS compliance process, how well you're doing and what percent of the SAQ is complete.

### Comprehensive support gets your questions answered

Have a question? With our built-in help, guides and security expertise, we can answer any PCI questions you may have – online, and via chat, email and phone.

### Integrated and automatic scans help ensure PCI DSS compliance

Once you set up a scan for the first time, the PCI Rapid Comply solution will automatically execute quarterly scans for those merchants that are required to pass a scan as part of the compliance process – there is nothing to remember to make sure these scans are completed.



## 96% not PCI Compliant

In 2011, 96% of the 855 data breaches investigated by the U.S. Secret Service and Verizon's forensic analysis unit involved merchants who were not compliant with PCI DSS at the time of the data theft.<sup>2,3</sup>

## 95% of data theft hits small merchants

Visa Inc. estimates about 95% of the credit-card data breaches it discovers are on its smallest business customers.<sup>4</sup>

*PCI security requirements apply to all merchants who handle payment card data during a transaction. If you accept credit card payments by any means, then you need to be compliant with PCI DSS.*

## 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.

## What Happens If I Don't Become PCI Compliant?

If your business fails to become PCI compliant<sup>3</sup>, you could be putting your business at greater risk from the growing threat of payment card data breaches and theft, which may result in substantial penalties (such as fines from banks, regulatory agencies, and card associations), fraud and charge backs, as well as legal costs and lost customers.

If your business experiences a data security breach, you could even lose your ability to process credit card payments. Perhaps more importantly, you risk the loss of customers. Research shows that 43% of customers who have been victims of fraud stop doing business with the merchant where the fraud occurred.<sup>5</sup>

## How can I learn more about PCI DSS compliance?

Please visit any of the following Web sites for additional information about PCI DSS:

- PCI Standards Council - [PCISecurityStandards.org](http://PCISecurityStandards.org)
- Visa - [usa.visa.com/merchants/risk\\_management/cisp\\_merchants.html](http://usa.visa.com/merchants/risk_management/cisp_merchants.html)
- MasterCard - [mastercard.com/us/sdp/index.html](http://mastercard.com/us/sdp/index.html)

## Do I have to use the PCI Rapid Comply<sup>SM</sup> solution?

The benefits of using the First Data® PCI Rapid Comply solution are that it is offered by and integrated with your Merchant Services provider. The PCI Rapid Comply solution includes a guided, step-by-step SAQ tool help to complete the annual questionnaire with ease, an integrated scanning tool for merchants that are required to pass quarterly scans and comprehensive support available online and via chat, email and phone to ensure your questions get answered.

As your service provider, we hope you will elect to use our PCI Rapid Comply solution. However you are free to obtain PCI DSS compliance services from third-party vendors.

If you choose to use a 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 for PCI DSS compliance services, you still will need to pay the Compliance Service Fee charged to you by your merchant services provider. The Compliance Service Fee is not affected by your choice to use a third-party vendor. You will also need to ensure your PCI DSS compliance status is reported to First Data. If you fail to become PCI DSS compliant or to report your PCI DSS-compliant status with a third-party vendor to First Data, you may also be charged a monthly non-receipt of PCI Validation fee by your merchant services provider until such time as you become PCI DSS-compliant or report your PCI DSS-compliant status to First Data.



## Layered Security with the First Data® TransArmor® Solution

Cardholder security is our first priority at First Data and the PCI Rapid Comply solution is just one of the many layers of security First Data offers. While maintaining PCI DSS compliance and adhering to the security standards goes a long way towards protecting your business and your customers, it does not remove cardholder data from the payment transaction process.

The First Data® TransArmor® solution is a multi-layered security solution that uses both encryption and tokenization technology to protect data in transit and at rest pre- and post authorization. The TransArmor solution protects against the theft or exposure of sensitive payment card data from the point of swipe through the storage in back-end systems.

The TransArmor solution combined with a sound PCI security strategy is a powerful combination to protect payment card and other sensitive data.

For more information, contact your Sales Representative or visit [firstdata.com](http://firstdata.com).

1. Merchants are responsible for valid answers to all questions whether or not they are prepopulated 2. Verizon 2012 Data Breach investigations Report, March 2012 3. Achieving PCI DSS compliance does not prevent a data security breach or compromise, or change the allocation of risk under your merchant agreement. 4. "Hackers Shift Attacks to Small Firms", Geoffrey A. Fowler and Ben Worthen, The Wall Street Journal Digital Network, July 21, 2011, <http://online.wsj.com/article/SB10001424052702304567604576454173706460768.html> 5. Javelin Strategy and research June 2009