Payment Card Industry Data Security Standard

Understanding What’s at Risk

Businesses not in compliance with the Payment Card Industry Data Security Standard (PCI DSS) risk substantial fines for data compromise and security breaches, as well as fees associated with non-compliance. Fines can exceed $1 million ($500,000 per association, per incident). In addition, merchants can be liable for the reimbursement of fraud losses and costs of reissuing cards—which could add up to millions of dollars.

What You Can Do

Merchants are required to perform a review of their data security practices. It is important that you check your card acceptance system to ensure it is not using any of the following:

- Payment applications that store prohibited track data
- Mon-compliant service providers
- Any other element expressed in the PCI DSS requirements that may prevent compliance

You may want to assess your risk and validate compliance with the assistance of approved security assessor/scan vendors. To help you navigate through the compliance process, First Data has contracted with www.securitymetrics.com, a scan vendor approved by Visa and MasterCard. This program provides online PCI self-assessment questionnaires, quarterly network scans (if applicable) and other significant benefits.

To schedule a review or a scan with SecurityMetrics, you may contact them at 801.724.9600 or www.securitymetrics.com. There are many other approved vendors which you can choose as a partner in achieving compliance, as well.

The following Web sites contain information to help you understand PCI DSS requirements and how to comply:

- www.SecurityMetrics.com
- www.YourMerchantInfo.com/pci
- www.PCISecurityStandards.org
- www.Visa.com/cisp