Payment Card Industry Data Security Standard (PCI DSS)

In this electronic age, customer account data has become a growing target for fraudsters. You often hear about the high profile cases that involve millions of credit card numbers being stolen or compromised. What you don't hear about is the vast majority of breaches that affect small and medium sized businesses. One of your key tools in the fight against such crimes is your full participation in, and compliance with the Payment Card Industry Data Security Standard (PCI DSS).

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

The five major card networks (*Visa* Inc., MasterCard Worldwide, American Express, Discover Financial Services and JCB) established the PCI DSS as a set of requirements for businesses of all types to use when configuring their IT and payment-processing environments. Understanding the requirements is the first step. Some businesses will need IT support to ensure all of the requirements are met prior to taking action to certify compliance. For additional information, please visit **pcisecuritystandards.org**

Protecting cardholder information is everyone's job. It's an investment that can benefit your business in a number of ways:

- Protects your brand's reputation
- Reduces fraud and losses
- Mitigates unnecessary expenses
- Builds customer loyalty by increasing the confidence of your customers
- Attracts new security-conscious customers

Begin certification today by visiting **tdmerchantservices.com/pci4**

What does a business need to do to certify as PCI DSS compliant?

Businesses must complete the following two steps (if applicable) to validate that they have achieved PCI DSS compliance certification:

Self Assessment Questionnaire (SAQ)	Most businesses are required to assess their own IT and payment processing environment using the appropriate PCI SAQ. Please see the PCI Security Standards site for examples of the five questionnaires by visiting: **pcisecuritystandards.org/merchants/self_assessment_form.php**
Vulnerability Scanning	Depending on how you process payments, network vulnerability scanning may also be required, which requires the involvement of an Approved Scanning Vendor (ASV).

Trustwave
Security begins with Trust℠

TD

TD Payment Card Industry Level 4 Program

Working with Trustwave (a PCI-certified Qualified Security Assessor), TD Merchant Services will ensure that you are provided with PCI compliance tools and data security solutions to help you meet the requirements for PCI DSS. As a TD Merchant Services customer, your PCI Security Fee will give you access to the Self-Assessment Questionnaire (SAQ) and Vulnerability Scanning services which Trustwave, an ASV, offers with TrustKeeper. This program is designed for merchants who are annually processing less than 20,000 ecommerce transactions or less than 1,000,000 transactions via all other processing channels.

TrustKeeper benefits include:

Easy Set-Up	The PCI Wizard guides you through the required steps for your business type.
Resources for your staff	Access to a number of PCI resources, including: PCI Video Assistant, on-line help text, tutorial, and other reference materials.
Your own PCI Best Practices	With the Security Policy Advisor, you can develop your own unique internal best practices, and comply with PCI DSS policy requirements.
Peace of Mind	With Vulnerability Scanning you can help to secure your website or store.

The certification process is easy!

Visit us at **tdmerchantservices.com/pci4** and click 'Get Started'. Then choose the PCI Wizard to help take you step-by-step through the process, beginning with how you accept credit cards, and identifying any steps you can take to protect your business.

For additional assistance enrolling, contact Trustwave at 1-877-815-4515.