

# Why Your Business Should Be PCI Compliant

At TransFirst®, we know security is an important issue for you and your customers. A breach can cost you and your company not only millions of dollars but also peace of mind. This doesn't even count the hidden costs such as loss or damage to your brand. We understand these fears and are committed to delivering the most secure payment processing services to you.

For the last seven years, we have followed the Payment Card Industry Data Security Standard (PCI DSS) and Cardholder Information Security Program (CISP) guidelines to help our merchants continue to grow, succeed and preserve their image as a trusted vendor. The PCI DSS is a security requirement designed to help organizations protect customer account data on a global basis.

Unfortunately, no one is safe from a data breach. In fact, according to the Identity Theft Resource Center the number of data breaches rose nearly 50 percent in 2008. By following the PCI DSS procedures, you and your business will be better prepared to secure your customers' personal data, thereby, increasing customer self-assurance, protecting your business from financial losses and remediation costs, and preserving the reputation of your brand.

These standards for security management, policies, procedures, network architecture, software design and other protective measures are summarized below. These regulations apply to all merchants that accept, transmit or store any cardholder data, regardless of size, wealth or number of transactions.

## **Build and Maintain a Secure Network**

- Install and maintain a firewall configuration to protect data

- Do not use vendor-supplied defaults for system passwords and other security parameters

## **Protect Cardholder Data**

- Protect stored data

- Encrypt transmission of cardholders' data sensitive information across public networks

## **Maintain a Vulnerability Management Program**

- Use and regularly update anti-virus software

- Develop and maintain secure systems and applications

## **Implement Strong Access Control Measures**

- Restrict access to data by business need-to-know

- Assign a unique ID to each person with computer access

- Restrict physical access to cardholder data

## **Regularly Monitor and Test Networks**

- Track and monitor all access to network resources and cardholder data

- Regularly test security systems and processes

## **Maintain an Information Security Policy**

- Maintain a policy that addresses information security

Under PCI, merchants fall into one of four levels based on VISA or MasterCard transactions volume over a 12-month period. Transaction volume is based on the aggregate number of VISA or MasterCard transactions (inclusive of credit, debit and prepaid) from a merchant Doing Business As ('DBA'). The merchant levels defined by VISA and MasterCard are summarized below:

### Level 1

Any merchant – regardless of acceptance channel – processing over 6 Million VISA or MasterCard transactions per year.  
Any merchant that VISA or MasterCard, at its sole discretion, determines should meet the merchant requirements to minimize risk to their system.

### Level 2

Any merchant – regardless of acceptance channel – processing 1M to 6M VISA or MasterCard transactions per year.

### Level 3

Any merchant processing 20,000 to 1M VISA or MasterCard e-commerce transactions per year.

### Level 4

Any merchant processing fewer than 20,000 VISA or MasterCard e-commerce transactions per year, and all other merchants – regardless of acceptance channel – processing up to 1M VISA or MasterCard transactions per year.

To guarantee that all credit card information is maintained in a secure environment, we ensured our Data Breach Security Program is PCI DSS compliant. You can always be assured TransFirst is PCI compliant by visiting VISA's website at [www.visa.com/cisp](http://www.visa.com/cisp).

This insurance program, which is offered on several of our products and services, covers a mandatory forensic audit required by the Payment Card Industry Data Security Standard (PCI DSS), card replacement costs and related expenses, and PCI DSS assessments and fines levied resulting from such a breach, regardless of your business's size.

Adopting PCI DSS may have additional costs associated with it, but the expenses are even greater if you choose not to abide by these guidelines. The cost of a data breach for a Level 4 merchant averages \$36,000 - in other words, more than enough to destroy a small business.

Data breaches can happen to any business, regardless of size. At TransFirst, we are here to help and arm you with the most cost-efficient tools, knowledge and support to ensure that your customers' data is protected.



**Trust. Innovation. Collaboration. - TransFirst.**

