Your Guide to PCI Compliance
On the surface, mandatory PCI compliance may seem complicated, even burdensome or intrusive, in the way you run your business. But think of it this way: PCI compliance equates to security for both you and your customers. Isn’t a little effort and diligence on your part a small price to pay for peace of mind when your livelihood is at stake?

What is PCI Compliance?
Simply stated, PCI compliance is adherence to PCI DSS, the acronym for Payment Card Industry Data Security Standards, which are administered by the Payment Card Industry Security Standards Council (PCI SSC). This independent group was established in 2006 by the five major payment card brands — Visa®, Mastercard®, Discover®, American Express® and JCB — to manage security standards for electronic transactions. Those standards, and additional information about the PCI SSC, can be found on the organization’s [website](http://www.pcisecuritystandards.org).

The PCI SSC publishes updated versions of the PCI DSS as needed. The PCI SSC helps keep the focus on raising awareness of security issues related to credit card payments. It also emphasizes that secure credit card processing is a responsibility shared by merchants, credit card processors (including TSYS®), card issuing banks and the credit card companies.

Although the PCI Security Standards Council does not impose consequences for non-compliance with its data security standards, the individual payment brands can and do impose fines and/or operational sanctions. Those penalties could be disastrous for your bottom line and your reputation with acquirers, payment brands and customers. Additionally, many states already have PCI compliance laws on their books, and more are expected to follow.

Secure Data Management
The comprehensive operational and technical requirements laid out in the PCI DSS establish consistent measures for data security management, policies and procedures, network architecture and software design. Businesses and merchants are required to process, store and transmit payment cardholder data in compliance with these requirements so that it is kept private and secure. Cardholder data is defined as any personally identifiable information associated with a cardholder including an account number, expiration date, name, address and Social Security number.
“Since online transaction and credit card fraud continue to be major threats to all businesses, PCI compliance remains critical.”

Since online transaction and credit card fraud continue to be major threats to all businesses, PCI compliance remains critical. That’s why it’s required of all entities with a Merchant ID (MID), from the largest Big Box stores to the smallest Mom and Pop shops and everything in between.

Think of PCI compliance as an ongoing process, not a one-time event in your business life. It is a series of common sense, “best practices” steps that all merchants and service providers need to incorporate as part of their security strategy.

**PCI Compliance Requirements**

The exact PCI compliance requirements for your company or business are available from your merchant services provider. TSYS provides general information about PCI compliance requirements [here](#).

Understanding the basis for PCI DSS will go a long way towards dispelling any concerns you may have about the process. Fundamentally, PCI DSS establishes six basic principles based on twelve core requirements (think of them as the “Digital Dozen”):

- **I. Network Security**
  1. Install and maintain a firewall configuration to protect cardholder data.
  2. Do not use vendor-supplied defaults for system passwords and other security parameters.

- **II. Data Protection**
  3. Protect cardholder data.
  4. Encrypt transmission of cardholder data across open, public networks.

- **III. Vulnerability Management**
  5. Use and regularly update anti-virus software.
  6. Develop and maintain secure systems and applications.

- **IV. Access Control**
  7. Restrict access to cardholder data based on need-to-know status.
  8. Assign a unique ID to each person with computer access.
  9. Restrict physical access to cardholder data.

- **V. Monitoring and Testing**
  10. Track and monitor all access to network resources and cardholder data.
  11. Regularly test security systems and processes.

- **VI. Information Security**
  12. Establish and maintain a policy to address information security.
The Four Levels of PCI Compliance
There are four levels of PCI compliance. Your particular level is determined by the number of electronic transactions you process annually.

Level 4
Small businesses — those processing less than 20,000 e-commerce transactions and less than 1 million other transactions annually — fall into this category. Level 4 businesses must complete an annual risk assessment using the appropriate PCI Self-Assessment Questionnaire (SAQ).

Level 3
Mid-sized companies generating between 20,000 and 1 million transactions annually require an annual risk assessment using the appropriate SAQ.

Level 2
Companies at this level handle between 1 million and 6 million transactions annually. A PCI SAQ must be completed each year.

Level 1
“Big Box” stores and other major corporations with a minimum of 6 million transactions per year must conduct an annual internal audit with a qualified PCI auditor.

Quarterly PCI scans, administered by an approved scanning vendor, may also be required for businesses at all four levels.

Whatever your level, TSYS’ Transaction Express® can reduce your PCI burden and help you achieve and maintain compliance by enabling you to easily accept payments with maximum security. This web-based payment gateway’s secure processing platform is fully PCI compliant and ideally suited for merchants of all sizes.

Transaction Express’ features and services are designed to meet your unique needs and expectations. For example, through its tokenization service, the gateway’s hosted payment page eliminates the need to store card data altogether by sending back only minimal information such as transaction and reference IDs and an authorization code.

PCI Compliance Means Security
By fully complying with PCI DSS, you can significantly decrease your risk of electronic data fraud that could seriously jeopardize or damage your business brand, reputation and finances. Just one data breach can cause a cascade of lost sales, cancelled accounts, destruction of business and community relationships, high-stakes lawsuits, insurance claims, and expensive fines and sanctions by individual payment brands.

As a merchant, you know that doing business is based on trust between you and your customers. Consumers who believe their sensitive credit or debit card information is safe with you are more likely to return and to refer other business your way. PCI compliance helps to establish that important level of trust and feeling of security.
Final Thoughts on PCI Compliance

Compromised electronic data negatively affects everyone involved: merchants, consumers, credit card processors, financial institutions and payment card brands. By achieving PCI compliance for your company or business, you’re taking responsibility for creating a first line of defense that will keep the data entrusted to you safe from fraudsters and thieves.

The protective measures outlined in PCI DSS are an investment in the global battle against electronic fraud. PCI compliance helps to ensure safeguarded payment card data with every transaction. Isn’t that what you and your customers expect?

When you’re ready to achieve and maintain PCI compliance, TSYS can help. Let one of our representatives answer your questions about credit card processing, merchant accounts, merchant services and PCI-compliant equipment, and then set you on the path to PCI DSS compliance.