globalpayments
Integrated

Guide to PCI Compliance

On the surface, mandatory PCI compliance may seem complicated, even burdensome or intrusive. However, PCI compliance equates to security for both ISVs and their merchants.

What is PCI Compliance?

Simply stated, PCI compliance is adherence to the Payment Card Industry Data Security Standards (PCI DSS), which are administered by the Payment Card Industry Security Standards Council (PCI SSC). This independent group was established in 2006 by five major payment card brands to manage security standards for electronic transactions. Additional information about the PCI SSC can be found on the organization's website.

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, ISVs, credit card processors, 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 card brands may charge fines if non-compliance leads to a security breach. Those penalties could be financially disastrous for ISVs and their merchants, as well as their reputations with acquirers, card brands and customers. Additionally, many states already have PCI DSS 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 who process, store and transmit payment cardholder data must do so in compliance with these requirements so that the data 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 potential online transaction and credit card fraud continue to be major threats to all businesses, PCI DSS 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.

PCI DSS compliance is an ongoing process, not a one-time event. It is a series of constantly evolving best practices that all ISVs and merchants need to incorporate as part of their security strategy.

PCI DSS Requirements

Understanding the PCI DSS requirements is important. Fundamentally, PCI DSS establishes six basic principles based on twelve core requirements:

I. Build and maintain a secure network.
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. Protect cardholder data.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.

III. Maintain a vulnerability management program.
5. Use and regularly update anti-virus software or programs.
6. Develop and maintain secure systems and applications.

IV. Implement strong access control measures.
7. Restrict access to cardholder data by business need to know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.

V. Regularly monitor and test networks.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.

VI. Information Security
12. Maintain a policy that addresses information security for all personnel.

The Four Levels of PCI Compliance

There are four levels of PCI DSS compliance for merchants. The level a merchant falls into is determined by the number of electronic transactions the merchant processes annually, and also determines the appropriate PCI Self-Assessment Questionnaire (SAQ) the merchant is required to complete.

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

Whatever your merchants' level, Global Payments Integrated can help reduce PCI scope as well as help achieve and maintain compliance by enabling them to easily accept payments with maximum security. In addition, our dedicated compliance services team focuses specifically on PCI issues and on providing your merchants the right assistance exactly when they need it.

PCI Compliance Means Security

By fully complying with PCI DSS requirements, you can significantly decrease the 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.

Further, your merchants know that doing business is based on earning trust from their customers. Consumers who believe their sensitive credit or debit card

information is safe with a merchant are more likely to return and to refer other business to that merchant. PCI DSS 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: ISVs, merchants, consumers, credit card processors, financial institutions and payment card brands. By achieving PCI DSS 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.

When you're ready to achieve and maintain PCI DSS compliance, we can help. Contact us today and 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.