6 Questions to Understanding PCI Compliance

By Kevin Gainer, Chief Sales Officer at CardConnect

When you boil it all down, PCI compliance is about doing what is right for your customers and maintaining their trust. Any good business wants to keep its systems secure and safeguard customers' payment information. Unfortunately, the process and standards for keeping this sensitive data safe continues to become increasingly complex and require more resources.

In coming weeks, CardConnect will be diving into the area of PCI compliance and what businesses should be doing to proactively address potential security vulnerabilities. Although, before we dive deeper, let's have a quick look at general questions related to PCI compliance.

1) What is PCI compliance?

Any company that processes, stores or transmits payment cardholder data must adhere to a set of standards known as PCI DSS – the Payment Card Industry Data Security Standard.

Cardholder data refers to the personally identifiable information (PII) associated with the owner of a debit, credit or pre-paid payment card. PCI compliance is how the Payment Card Industry Security Standards Council (PCI SSC) ensures merchants handle cardholder data in a secure environment.

All merchants who accept cards as payment for goods or services must be PCI compliant or risk financial penalties.

2) Which businesses are required to comply with PCI standards?

Any debit, credit or pre-paid card associated with any of the five members of the PCI SSC – American Express, Discover, JCB, MasterCard and Visa – falls under the scope of PCI compliance.

So, all merchants who accept card transactions by any mechanism – from point-of sale swipe terminals to e-commerce shopping carts – need to meet and maintain some level of PCI compliance criteria. This level is typically related to transaction volume.

3) How does transaction volume affect a merchant's need to be PCI compliant?

PCI compliance is required of all card-accepting merchants, regardless of the size or number of card transactions. But the transaction volume does impact which level of compliance each merchant is subject to.

Merchants fall into one of four validation levels based on their annual card transaction volume. The larger the business, the higher the validation level, and thus the higher the compliance requirements.

- **Level 1 –** Any merchant processing more than 6 million card transactions annually
- **Level 2 –** Any merchant processing 1 million to 6 million card transactions annually
- **Level 3 –** Any merchant processing 20,000 to 1 million e-commerce transactions annually
- **Level 4 –** Any merchant processing less than 20,000 e-commerce transactions and up to 1 million card transactions annually

Merchants who have suffered a breach that compromised cardholder data may be bumped up to a higher validation level. For example, a Level 2 merchant that experiences a breach may be moved (at the discretion of the card brand) to Level 1, which, in turn would introduce a more stringent level of compliance.

4) What steps must every merchant take to meet PCI compliance?

There are 12 categories of PCI DSS requirements that all merchants must meet in order to be considered compliant or they risk financial penalties imposed by the card brands. These categories provide a framework comprised of more than 275 questions and requirements and are dependent upon the Level indicated above as well as the role each party plays in the transaction process. The 12 categories are listed below:

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**
3. **Protect stored cardholder data**
4. **Encrypt the transmission of cardholder data across open, public networks**
5. **Use and regularly update anti-virus software or programs**
6. **Develop and maintain secure systems and applications**
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**
10. **Track and monitor all access to network resources and cardholder data**
11. **Regularly test security systems and processes**
12. **Maintain a policy that addresses information security for all personnel**

5) How do third-party payment processors help merchants reach PCI compliance?

Outsourced payment processors do not automatically provide compliance, however strong and resourceful partners like CardConnect can help merchants simplify ongoing compliance needs and rest easy knowing they're meeting all 12 requirements.

Hackers are growing smarter and more relentless every day. A third-party processor can reduce a merchants' risk of exposure and serve as an ongoing security consultant. Processors can identify system vulnerabilities that could be targeted by cyber criminals seeking access to a merchant's private network. They also should have expert knowledge on the latest compliance rules, as well as a pulse on new and customizable technologies that can decrease or remove a merchant's system from the scope of PCI compliance.

6) What are the risks of not being PCI compliant?

PCI DSS is a set of standards, not laws, but almost every state has enacted legislation requiring merchants to notify their customers of security breaches. Current state and federal privacy regulations forbid merchants from storing unencrypted cardholder data, PIN numbers as well as other PII.

Merchants who do not comply with PCI standards risk being subject to costly consequences – fines, legal fees, card replacement costs, forensic audits, decreases in stock equity, reputation damage and loss of business.

*For more helpful articles about the ins and outs of the payments industry, visit **cardconnect.com/blog**.*