A VertMarkets Publication

Retail Solutions Online

www.retailsolutionsonline.com 2008

# PCI Compliance: Keep Your Customers And Business Secure

Apparel and home fashion giant TJX Companies Inc. is still suffering from the fallout caused by the well-documented computer breach that compromised the identity of thousands of credit and debit card holders in January 2007. In addition to $150 million in breach costs, the company faces more than a dozen lawsuits, some of which are seeking tens of millions of dollars in damages. Worse, its reputation has suffered among consumers who frequent the company's network of national discount retailer stores.

By P. Gayle Hoskinson, Interchange and Compliance Manager, Heartland Payment Systems

The threat of a data breach is a reality for all retailers, and as a result, safeguarding customer data should be a top priority. To make sure it stays a priority, the PCI Security Standards Council – an independent organization formed by Visa, MasterCard, American Express, Discover Financial Services, and JCB International – developed the PCI Data Security Standard (PCI DSS), a set of guidelines to help retailers minimize fraud and make sure their credit and debit card processing is secure.

The PCI DSS provides steps to protect organizations, customers, and the card processing system from fraud. The steps include requirements for security management, payment policies, data storage procedures, network architecture, software design, and other payment system measures.

These guidelines are not merely suggested reading for retailers. While the council develops and maintains the standards, each card company independently implements and enforces those standards. In 2006, they leveled fines totaling some $4.6 million to card processors of non-compliant retailers around the country, and these fines were passed directly to the retailers.

For retailers accepting credit or debit cards branded by any of the five major card companies, the message is simple: You are required to uphold and comply with the PCI DSS. Failure to do so may result in fines, even without evidence that your system was compromised.

In the past, card companies did not enforce PCI DSS equally across the board; as such, it was overlooked by smaller merchants and their card processors. However, that is no longer the case. Visa recently announced a five-phase approach to eliminate the use of non-secure payment applications for all merchants. In short, this means all retailers, regardless of their size, need to address security issues immediately.

The good news is that it's not hard to avoid the fines. You simply need to understand the PCI DSS' six core principles and work with your card processor and other technology providers to meet the standards. If it still sounds daunting, consider this: it should be less overwhelming than a six-figure fine. Better still, staying PCI compliant protects your company and customers from fraud and also builds consumer trust.

### The Six Core Principles Of PCI DSS

Before you can become PCI compliant, it is important to first understand the six core principles of PCI DSS. Following are brief outlines of each principle.

#### *1. Build And Maintain A Secure Network*

Choose, install, and maintain an up-to-date network firewall, antivirus, and antispyware system. These programs close holes in your network that hackers can use to gain entry and steal cardholder data. And always change the default password for your programs, firewall, routers, computers, and other systems. This ensures that only authorized persons can log on to your various network resources. Hackers know every product's default password. Their first method of attack will be to try to access your network using these well-known login credentials. If you change all of your passwords, this type of attack will fail.

***2. Protect Cardholder Data***

Encrypt all transmissions across open, public networks. Encryption software is required for POS systems connected to the Internet for cardholder data transmission. Also, it is imperative that retailers only keep cardholder data that is essential to the business, such as receipts and reports. Sensitive information, such as magnetic stripe data or card validation codes, should never be stored beyond what is required for business, legal, or regulatory purposes.

***3. Maintain A Vulnerability Management Program***

If you are using a credit card payment software application or a POS terminal with a debit card PIN pad, you should ask your card processor to verify PCI compliance and request an upgrade on outdated equipment or applications. Dated systems without proper software face an exponentially higher risk for network breaches and data theft. Also, update all of your core security applications on a regular basis. That includes firewalls, antivirus, antispyware, operating systems, and business applications. You can ensure your card processing equipment is up to snuff by checking the Visa List of Validated Payment Applications online at www.visa.com/cisp.


For retailers accepting credit or debit cards branded by any of the card companies in the PCI Security Standards Council, the message is clear: Comply with the PCI DSS, or face potentially steep fines.

***4. Implement Strong Access Control Measures***

Only allow the most senior company officials to have access to cardholder data. Protect access by issuing user IDs and passwords and assigning access control rights through your network. Make sure anyone who will have access to cardholder data has had a background check performed and does not have a criminal record. Lastly, delete logins and update all company passwords when an employee leaves the company.

***5. Regularly Monitor And Test Networks***

This includes computers, POS systems, and anything storing or processing cardholder data. Maintain tracking records to demonstrate your security systems and processes are regularly tested and validated.

***6. Maintain An Information Security Policy***

Document and maintain an enforceable policy that addresses details of information security. All employees handling sensitive information should know and understand the rules.

If any one of your technology providers doesn't step up to help you maintain compliance with these six principals, it's time to take charge and demand they do so – or change vendors. Even if your payment application is the cause of a breach in security, it's your name and corporate bank account on the line.

**Staying Compliant**

Staying compliant protects customers from fraud, ensures customer satisfaction and trust, and helps you avoid substantial fines for not being up to code, whether or not there is a security breach.

Be sure to work with a PCI Approved Scanning Vendor (ASV) to perform quarterly vulnerability assessment scans to probe your card payment systems. These scans test all public IP addresses involved in card acceptance, transmission, and storage. Check with your card processor, as most have a relationship with at least one ASV who can help you become compliant.

During testing, ASVs grade system vulnerability on a scale from highly secure to highly vulnerable. If a system is graded at a lower level, it will fail the PCI scan report.

You will then have a specified amount of time to update your systems and make them compliant with PCI DSS requirements. If they remain non-compliant, you face fines – from $1,000 to $500,000 per incident – and possible expulsion from card acceptance programs.

The situation worsens when a breach occurs and your network is not PCI DSS compliant. Fines increase substantially per incident, and you may be held responsible for a portion – or all – of the cardholder losses. Further, if you fail to report a suspected or confirmed breach, you are subject to an additional penalty of $100,000 per incident.

As a result, ensuring your payment system is PCI DSS compliant could be the most important thing you do as a business owner or manager. A compromise can cost you your reputation, your customers ... even your business.

**Are You PCI Compliant?**

You can find out if you are compliant by taking the required PCI DSS Annual Self-Assessment Questionnaire, which is available on the PCI Security Standards Council Web site at www.pcisecuritystandards.org. (The site also includes a list of ASVs.) Next, make sure your card processor is serious about the security of your business and your customers. If your card processor is not committed to compliance with these standards, it is time to look for a new one.

**About The Author**

P. Gayle Hoskinson is the interchange and compliance manager at Heartland Payment Systems, a provider of credit/debit/prepaid card processing, payroll, and payment services to more than 150,000 small and mid-sized businesses nationwide. Heartland Payment Systems is the founding supporter of The Merchant Bill of Rights, a public advocacy initiative that educates merchants about fair credit and debit card processing practices. For more information, visit www.merchantbillofrights.com. ◆