

By Andrew Sanders

Ensuring Credit Card Security via PCI Compliance One Year after the Deadline

More than a year ago the credit card companies came together to create a security standard, called the Payment Card Industry (PCI) Data Security Standard, that was mandatory for merchants that use credit card transactions. By June 2005, nearly all businesses that process credit card transactions were required to have achieved PCI compliance.

It's not surprising that this standard was

put in place, as credit card security is a hot topic in the era of the Internet and paperless financial transactions. According to one recent study, the total fraud amount in 2006 was approximately \$56.6 billion, and the mean fraud amount per fraud victim rose in the same year to \$6,383¹—significant costs for the significant problem of credit card security. More than 10 million people per year are affected by identity theft, and in 2005 at least 152 data disclosure incidents have been disclosed, potentially affecting more than 57.7 million individuals.²

In 2001, Visa cre-

ated a program known as the CISP (Cardholder Information Security Program) that was meant to heighten credit card security with merchants using the Visa brand. Eventually this credit card security program was expanded and embraced by all major credit card companies, including MasterCard, Discover and American Express. Merchants were required to have achieved PCI compliance by June 2005. However, even over one year after the deadline, not all merchants have been properly certified and may face fines or other penalties. At one point recently, Visa reported that 83 percent of 231 large merchants

had not yet established PCI compliance, and that while approximately 75 percent filed initial reports regarding initial steps toward compliance, 8 percent had not filed a report at all.³

The problem arises when merchants are not aware of the need for PCI compliance and therefore do not become certified. For example, hotels that exist on the campuses of universities are considered to be a part of those universities. As a result, such hotels are looked at as having a large number of yearly transactions when combined with those of the universities, even if the hotels themselves do not fit one of the higher merchant categories on their own. These hotels may have previously dismissed the need for PCI compliance, but they are now being reviewed closely and may be facing large fines for the oversight, particularly if they have had issues with credit card security in the past. In the next few years, mid- and large-sized hotel chains are going to find that they are being scrutinized for the measures they have taken to ensure credit card security, and that any vendors with which they are involved also need to be certified.

Hotels may incur fines if a breach in credit card security occurs while they have not yet achieved PCI compliance. While the cost of PCI compliance—or of hiring a consultant to become compliant—may at first seem higher than the cost of the fines themselves, the credit card companies are starting to levy additional penalties that could be detrimental to a business. For example, Visa USA states that if a business fails to comply with requirements or fails to rectify a security issue, Visa may fine the responsible member or impose restrictions on the merchant or its agent.⁴

In fact, the credit card companies have been scrutinizing the process themselves, and have been making changes to increase credit card security that could affect your business. Visa USA recently reclassified level four merchants (merchants that process fewer than 6 million credit card transactions a year) as level two, which requires additional scans and forms. Those that have been reclassified now have until September 30, 2007, to demonstrate compliance⁵. Changes such as this mean that even if your business is already compliant, you

need to make sure you have accurate information in order to stay current.

The bottom line is that PCI compliance is an important issue that is not going away. It is critical for hotels to make sure that they are compliant, either by using internal resources or by hiring a consultant. The credit card companies are continuing to pay close attention to this standard, and businesses that are not compliant face more than just fines, they may lose customer confidence—particularly if a security breach occurs. There's no more time for excuses—if you're not working toward PCI compliance, make sure you start the process immediately.

Andrew Sanders is director of sales and marketing for RedSky IT, based in New Jersey.

The deadline for businesses to achieve PCI compliance has now passed. Is your business compliant?

- If your answer is yes, fantastic. Keep doing what you're doing, and make sure that you're up to speed on the latest changes introduced by the credit card companies.
- If your answer is that you're working on it, you're a bit late to the game. Most merchants were supposed to have reached PCI compliance a year ago.
- If your answer is "What are you talking about?" then it's time to get serious. The credit card companies won't listen to you if you plead ignorance.

Below is a brief overview of the requirements for PCI compliance.

1 Build and Maintain a Secure Network

All merchants, including hotels, are required to install and maintain a firewall within their computer systems to maintain credit card security and to protect sensitive information from being accessed by those outside of the system. In addition, merchants seeking PCI compliance must not use vendor-supplied defaults or system passwords. New passwords must be assigned to all systems and must be kept secure.

2 Protect Cardholder Data

Merchants must protect credit card security by encrypting the transmission of data across public networks. Any property management system used by the hotel must be secure as well.

3 Maintain a Vulnerability Management Program

Merchants must use and regularly update antivirus software and must develop and maintain secure systems and applications.

4 Implement Strong Access Control Measures

To ensure credit card security, the hotel must restrict data only to those who need to know the information. In addition, the hotel must assign a unique ID to each person with computer access for tracking purposes. And finally, the hotel must be sure to restrict physical access to cardholder data.

5 Regularly Monitor and Test Networks

The hotel must test and monitor access to network resources and cardholder data. Security systems and processes must also be tested regularly to guarantee credit card security.

6 Maintain a Good Security Policy

Merchants are required to have a documented process so that if there is an unfortunate breach in credit card security, there is a structured procedure to follow in order to address that breach.

¹ <http://www.privacyrights.org/ar/idthefts-surveys.htm>

² <http://www.pcicomplianceguide.org/pci-consumers.html>

³ <http://storage.knowledgestorm.com/ksstorage/search/viewabstract/83617/index.jsp>

⁴ http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

⁵ http://usa.visa.com/download/business/accepting_visa/ops_risk_management/changes_to_merchant_levels_bulletin.pdf