# Education (continued)

# The concern du jour? PCI

**By Ross Federgreen**
*CSRSI*

I recently attended the Southeast Acquirers' Association meeting in Jacksonville, Fla. While there, I spoke with a number of registered and nonregistered ISO owners and merchant level salespeople (MLSs). I wanted to ascertain their most pressing educational needs. To my surprise, they indicated their area of greatest confusion and concern is PCI.

So, here are answers to the top three questions they asked:

## What is PCI?

PCI is short for the Payment Card Industry Data Security Standard. It is also abbreviated PCI DSS. The current version of PCI is 1.1. It was promulgated in September 2006. The PCI Security Standards Council is the central reference source for rules and regulations relating to PCI.

PCI is the result of a combined effort of the card brands – including Visa U.S.A., MasterCard Worldwide, American Express Co., Discover Financial Services LLC and JCB International Co. Ltd. – to provide uniform data security standards and requirements.

Previous security programs such as the Visa Cardholder Information Security Program and MasterCard Site Data Protection program have been folded into PCI.

## Whom does PCI affect?

The short answer is everyone. It is critical to understand that merchants in both card present and card not present environments must meet PCI requirements. And *all* merchants who receive, transmit, store, manipulate or essentially touch cardholder data in any manner are affected.

Specific PCI requirements are driven by merchant categories, which were updated last year. Four distinct merchant designations range from level 1 (those who have the greatest security requirements) to level 4 (those who have the least regimented requirements).

Remember, both card present and card not present merchants must comply with PCI: No merchant is excluded.

Merchants are primarily pegged by their annual volume of e-commerce and traditional transactions. However, any merchant – at the sole discretion of any card brand – can be categorized a level 1 merchant. And merchants of any size or type who experience data breaches can also be declared level 1 merchants.

## What are the PCI requirements?

PCI contains a series of requirements that can be divided into two areas: annual self-assessment questionnaires (SAQs) and quarterly penetration scans. But this is only the beginning.

First, a merchant's level must be determined. The number and type of transactions merchants handle drive their category designations.

The next step is to find out if the mandated compliance date for the merchant's category has already passed. The best way to approach this is to act as though it has. In fact, all merchants at levels 1, 2 and 3 must be in full compliance now.

And, although there are some acquirer-specific exceptions for level 4, the safe answer is to assume all level 4 merchants should also be compliant right now.

Quarterly penetration scans need to be performed by an approved scanning vendor (ASV). The authority to approve an ASV rests with the PCI Security Standards Council. The list of the approximately 125 approved ASVs is at *www.pcisecuritystandards.org/pdfs/pci_asv_list.pdf.*

A number of ASVs tell merchants they need to have scans done more often than once per quarter. This is not true. They also say that in order for ASVs to do their work, merchants must provide completed SAQs to them. This is also not true.

Recommend to your merchants a company that is on the published ASV list. And tell your clients the ASV does not need access to their SAQs in order to do its job.

## Don't sack the SAQ

Every merchant must complete a SAQ annually. No exceptions. It consists of approximately 75 questions, which are designed to probe into merchants' actual working conditions.

Many merchants believe this is a meaningless exercise and think it does not matter whether they answer the questions accurately.

This could not be further from the truth. These documents and filings should be viewed in the same light as an

***It is critical to understand that merchants in both card present and card not present environments must meet PCI requirements.***

IRS 1040, except you cannot modify your SAQ results after the document is filed. Never allow merchants to fabricate or answer inappropriately.

Many merchants do not understand that they must file their SAQs with their service providers. They also do not realize that a single no answer in the questionnaire will put them out of compliance.

If a merchant does the annual self-assessment and answers no to one or more questions, the risk (or risks) causing the problem must be resolved. Then the merchant must retake the self-assessment to demonstrate compliance before submitting the SAQ.

The current version of the SAQ consists of 12 requirements in 64 major sections. In addition, many of the 64 sections contain subsections. To complete the SAQ, merchants must have a thorough working knowledge of PCI version 1.1, including its multiple nuances.

A common error merchants make is to give information technology (IT) departments or consultants responsibility for answering the SAQ or interpreting PCI.

The PCI and SAQ are not IT documents; they are business documents. This cannot be over-emphasized. Proper SAQ completion requires the expertise and perspective of senior management. Period.

A full understanding of PCI and a deep appreciation for the dynamic state of the issues involved will make you, as ISOs and MLSs, more valued partners to your customers.

As always, remember that knowledge is power.

*Ross Federgreen is founder of CSRSI, The Payment Advisors, a leading electronic payment consultancy specifically focused on the merchant. He can be reached at 866-462-7774, ext. 23, or* rfedergreen@csrsi.com.