



# Winning the PCI Compliance Race

*Upcoming deadlines push merchants, ISOs, processors, and acquirers toward compliance finish line*

By Richard H. Gamble

In the relentless campaign to secure sensitive cardholder data, industry players face a series of deadlines that affect not only merchants, but also ISOs, processors, and acquiring banks. This month, the first updated PCI standards since 2006 will be released, along with a deadline for bringing merchants new to accepting cards into compliance.

PCI data security compliance is “a marathon, not a sprint,” insists Martha A. Rhine, director of international association compliance at Global Payments Inc. in Atlanta. “And the end comes on July 1, 2010.” That’s when all merchants must be PCI Data Security Standard (PCI DSS) compliant or use a PABP/PA DSS-compliant POS system. This month, all newly boarded merchants will have to meet that same standard.

The bigger challenge looms in 2010, when no merchants will be able to process transactions through noncompliant POS terminals, says Barrie Berman VanBrackle, partner in the Washington, D.C., office of Manatt Phelps & Phillips LLP. Level 4 merchants (those with fewer than 20,000 e-commerce transactions, or fewer than one million total transactions each year with any card brand) are asked to fill out an annual self-assessment questionnaire and perform a quarterly network scan, she notes. Depending on the acquirer’s policy, the scan can be validated by the merchants or by a certified network scanner (one of a host of companies listed on the PCI Web site).

It has taken the better part of the last four years, since the PCI standard debuted, to achieve compliance among nearly all large (Level 1 and 2) merchants, and gain solid participation by Level 3 merchants, reports Michael Petitti, chief marketing officer at Chicago-based Trustwave. Level 3 targets primarily small e-commerce merchants, and that emphasis on e-commerce is paying off. “The Level 3 merchants have become pretty astute about protecting customer information,” Petitti says.



Level 4 includes 99 percent of the merchants that accept Visa card payments. So in many ways, all of the attention focused on Level 1 and 2 merchants to comply is just the tip of the iceberg, though it’s particularly important due to the high volume and high value of their transactions, VanBrackle says.

Getting the roughly 6 million Level 4 merchants to comply is a much more daunting task, Petitti points out. “In our forensic investigations of data breaches in the United States, the majority—probably nine out of 10—occur at small merchants doing card-present transactions,” he says. “There are still a lot of nonsecure POS systems out there, even after several years of considerable effort.”

## Strength Training

Finishing the compliance race now means shoring up weak spots. To identify them, Phil Neray, vice president of marketing at data security vendor Guardium Inc. in Waltham, Massachusetts, cites a recent Gartner report that described the three major challenges to PCI compliance: protecting and encrypting confidential consumer data stored on file servers or databases; finding ways to separate sensitive card data from other data on a merchant network and then limit and track access to that data; and encrypting data while it’s in transit.

Despite weaker compliance among the smallest merchants, the largest at-risk group is not merchants using terminals, but rather those using integrated POS systems, Rhine explains. Even with a PABP/PA DSS application, they still have compliance issues to address. “There’s still a risk of being compromised by viruses that can cause a breach and ruin a reputation,” she says. “Getting a PABP/PA DSS application is a great first step, but you still have to secure a PC that could be visiting Web sites and could get infected with spyware. And you need to stay current with security patches.”

Hackers have found that small merchants with PC-based POS systems connected to the Internet are the most vulnerable, Petitti reports. “Many older systems are still somewhat insecure,” he says. “But the industry has done a lot of work over the past five years. The contrast between then and now is like night and day.”

Still, the huge group of Level 4 merchants hasn’t been given a pass up to now. “They’re obligated to comply. They face the same sanctions as larger merchants, the same liability for breaches, and most likely, the same fines for noncompliance,” Petitti explains. The only official difference is that they are not required to validate compliance. That’s left up to the acquiring banks to enforce, and they are working with equipment vendors to

upgrade these merchants. "They're asking processors and resellers, 'Who in my portfolio hasn't been upgraded yet to compliant POS systems?' and going after them," he explains.

Getting many of them up to snuff may not be too difficult. Level 4 includes a large group of very small merchants that may actually find compliance fairly easy, says Michael Maloof, chief technology officer at TriGeo Network Security, a security information and event management vendor based in Post Falls, Idaho. "If they accept cards, don't store data, and use equipment for transmitting data supplied by their processor that is PCI compliant, they can sail through an audit," he says.

But even the low-tech merchant—one that takes paper imprints with old knuckle-buster manual equipment, for example—needs to be trained to destroy the paper slips after the data has been entered into a system, Neray adds.

### Penalties for Disqualifiers

The campaign to achieve PCI compliance involves some stiff consequences for noncompliance. When a breach occurs, the card brand will levy fines against the

merchant acquiring bank, VanBrackle explains. The bank will likely try to pass the fine on to the merchant, directly or indirectly. In some cases, the bank also would pass on the fine to a processor, which would pass it down the chain to an ISO, which would pass it on to the merchant, she explains. ISO liability entirely depends on contract language. Ultimately the fine is supposed to hit the entity that allowed the breach to occur.

The role of the ISO has evolved from pure sales to more ongoing responsibility for the merchants they sign up, explains card payments consultant Ali Raza, executive vice president of Speer & Associates in Atlanta. "They're more likely now to take a piece of the action and a piece of the risk, which means they're very much in the chain when it comes to PCI compliance for their merchants."

Merchants that showed they made a good faith effort to comply last year and confirmed that they did comply by Oct. 1, 2008, were able to collect three months' worth of the difference between the higher interchange they have been paying and the lower interchange offered for which they now qualify. "This is a way for mer-

chants to put money in their pockets in the form of a refund," Neray says.

In spite of rewards and penalties, an effective PCI compliance program requires a combination of well-trained people, good policies, and up-to-date technology. "You have to train people in best practices so they know better than to leave a spreadsheet with credit card numbers on a file server or share login names and passwords among themselves," says Neray. **TT**

*Richard H. Gamble is a contributing writer to Transaction Trends. Reach him at [gamble10@earthlink.net](mailto:gamble10@earthlink.net).*

### Mark Your Calendar: Compliance Day

For ISOs, processors, and acquirers who want to learn more about PCI compliance, ETA is sponsoring a Compliance Day event Nov. 5-6 in Dallas. Attendees will get a chance to hear from executives of all the major card brands as well as representatives from security firm TrustWave, NACHA, and the PCI SSC. They are expected to provide clarification about evolving PCI standards, compliance deadlines, liability for breaches, fines and penalties for noncompliance, and useful ways to help small merchants comply. Visit [www.electran.org](http://www.electran.org) for details.



"When making a good impression counts"™

*Count on Quality Imprinters  
and Merchant Plates  
From Data Systems.®*

Email:  
[Sales@DataSystemsCompany.com](mailto:Sales@DataSystemsCompany.com)

**(843) 856-1025**

The advertisement for USAePay features a background of a green golf course with a golf ball in the foreground. The USAePay logo is prominently displayed at the top, with "USA" in blue and "ePay" in white with a blue outline. Below the logo, it says "PCI Certified Payment Gateway" and "Verified Merchant by VISA SecureCode". The main headline reads "Get In The Green with USAePay" in a mix of green and red fonts, with the tagline "...Where Business is Done in Real Time..." underneath. A list of solutions follows, including eCommerce/Mo/To, Retail, Check Processing, Mobile Processing, Integrated Terminals - Exadigm, QuickBooks®, Multi-Currency Processing, and Satisfaction Guarantee Program. At the bottom, the phone number 1-866-490-0042 and the website www.usaepay.com are listed.