

# PUSH

Practical business realities force compromise when it comes to PCI standards enforcement

By Richard H. Gamble

## KEY NOTES

- ▶▶ While some ISOs are refusing to board new merchants unless they see proof of PCI compliance, they aren't taking that position with existing merchants.
- ▶▶ Insurance against data breaches has become a popular option. Most policies provide protection if a merchant made a good faith effort to comply and is still breached. They won't pay merchants that ignore compliance procedures.
- ▶▶ Merchants are more interested in protection than compliance.



# comes to **SHOVE**

**W**here PCI compliance is concerned, principle is colliding with practicality. Nearly everyone agrees that data security is important and that PCI standards are both helpful and come with mandates that can hardly be ignored. However, questions remain about the practical realities of how far small merchant operations will be forced to conform to the principles of PCI compliance—and how much those principles will have to bend to business realities.

Small merchants clearly are resisting. “Merchants’ faith in PCI is diminishing,” reports Cliff Gray, an associate of the Strawhecker Group. “They don’t think it’s meaningful. They don’t think it will keep them safe.” The path to PCI compli-

ance, he says, is to pitch security first and PCI compliance second. If they are persuaded to take prudent steps to secure their data, they may comply with PCI as well, but they’re more interested in protection than in complying with standards they see as being imposed from outside, he insists.

“I spoke with several ISOs at the recent ETA meeting, and they feel like they’re beating their heads against a wall,” Gray says. “They aren’t having much success, but they really aren’t trying new strategies yet. It just won’t happen until ISOs agree to refuse to board new merchants unless they are PCI compliant, and then they extend that same requirement to their existing portfolios.”

“There is no sure-fire solution to

achieve full merchant compliance,” adds Moneris USA President Greg Cohen. “It’s up to the merchants to comply and up to the acquirers to see that they do.” Neither is exactly stepping up to the plate. “We all know that if we don’t board a noncompliant merchant, a competitor might,” he notes. “Merchants that don’t want to comply will find the leaks in the system. That won’t change until we, as an industry, agree to shut a merchant off from card processing if it doesn’t comply.”

For merchants that choose to comply, the toolkit is robust, Cohen says, but upgrading or replacing a POS system to gain compliance can be expensive, and for many mom-and-pop shops, compliance just isn’t a high priority, he explains.



## Acquirers and ISOs are taking PCI compliance seriously. For an issuer, a data security breach is an operating expense. For an acquirer or ISO, it can mean losing your life's work.

—Marc Abbey, First Annapolis Consulting

### No Time for Passivity

ISOs are caught in the crossfire. While acquiring banks are the official enforcers of PCI, as a practical matter, it's the ISO that the merchant does business with and the ISO that causes the merchant to comply or not comply with all the card brand rules and regulations, Gray says. "The ISO's role is huge," he insists. But ISOs, with a few exceptions, take a pretty passive role when it comes to compliance, Gray notes. "They mail out statements about PCI and data security. They use monthly statement stuffers. They have all kinds of stuff on their Web sites. But I don't know of any ISOs that are taking an aggressive stance, which would be requiring merchants to prove they are PCI compliant or the ISO would cut off processing. Some ISOs are refusing to board new merchants, especially e-commerce merchants, unless they see proof of PCI compliance, but I don't know of any that are taking that position with existing merchants."

ISOs won't jeopardize a relationship by mandating PCI compliance, says consultant Les Reidl, president of Speer & Associates. When compliance depends on hardware and software that are PCI enabled, it tends to work pretty well. When it depends on getting merchants to change policies and procedures, you run into problems, he explains. Getting proper procedures embedded down to the sales clerk level can be a real challenge, he adds.

Not everyone sees the situation as a stalemate. "The Visa numbers show pretty good compliance for the Level 1, 2, and 3 merchants," says Michael Petitti, chief marketing officer at Chicago-based Trustwave. "Those numbers aren't anywhere near as good for Level 4 merchants," he concedes. Level 4 are the smallest merchants. There are millions of them (6 million in the U.S. alone), while there are just a few thousand of the larger merchants, but the large merchants account for two thirds of all card transactions

and quantitatively represent the greatest risk, so they got the highest priority and the earliest deadlines in the compliance push, he says.

### Two Deadlines Down, One to Go

Two deadlines issued by Visa are having real impact, Petitti says. One has already passed: As of Oct. 1, 2008, all Level 3 and 4 merchants had to be PCI compliant or be using a PADSS-approved application to be newly boarded. (PADSS stands for payment application data security standard.) The next big deadline is July 1, 2010, by which time all Level 3 and 4 merchants are expected to be PCI compliant or using a PADSS application. Theoretically, by next July, all card-accepting merchants, regardless of size, will have to be PCI compliant.

The deadlines do have teeth, and they will be effective at moving Level 4 merchants toward compliance, Reidl says, particularly the Visa July 1, 2010, deadline. But verifying compliance will be a practical compromise. "We'll see tangible results, but when compliance is self-certified and self-monitored, there are limits to how effectively it can be policed," he notes. The card brands will continue to use deadlines to manage overall program risk and accept the fact that there will be a few laggards, he says.

Acquirers and ISOs are taking PCI compliance seriously, insists Marc Abbey, a partner at First Annapolis Consulting. "For an issuer, a data security breach is an operating expense. For an acquirer or ISO, it can mean losing your life's work," he says.

Some resistance may disappear as deadlines get closer. A lot of ISOs and Level 4 merchants are not paying attention yet to PCI compliance because they don't have to, says consultant Paul Martaus, president of Martaus and Associates. "Everyone is aware of the deadlines, but not much will happen until the deadlines get closer," he predicts.

Petitti sees more progress. "Acquirers started by providing information, but they're getting more aggressive at mandating PCI compliance" for merchants to use any of the major card networks,

# PCI COMPLIANCE? NO PROBLEM.



## Simplify PCI

Wondering how to help your merchants become PCI compliant and keep them happy? SecurityMetrics can help. As the largest PCI-DSS vendor in the world, we've helped more merchants become compliant than any other vendor. Our simple approach works.

**Call today to receive a free consultation for your business. 801.705.5670**

[www.securitymetrics.com](http://www.securitymetrics.com)

securityMETRICS®

Petitti says. Even for small ISOs, requiring merchants to comply or lose network access is becoming a fact of life, he notes. The astute ISOs are offering ways to streamline compliance and using it as a selling point, he adds.

Most acquirers and ISOs now provide PCI compliance tools and materials and charge merchants for it, Abbey says.

To comply, Level 4 merchants will have to fill out one of five self-assessment questionnaires, the one that best fits their industry type, Petitti says. And they will have to have network scans on a regular basis. A scan is basically an electronic inspection to find out if any doors or windows are unguarded, he explains.

The waiting is over for TransPay Processing, a Palm Springs, California, ISO that is about to launch an aggressive campaign to get its merchants, all Level 4, to comply with PCI, reports Emil Billman, president. "We just signed a contract with ControlScan to contact our merchants—through outbound telemarketing in many cases," he explains. "We picked them over First Data, which is our processor, because we liked the ease of access to information that they provide. We'll be spending more than most ISOs, I suspect."

Billman expects some resistance on the part of merchants due to unfamiliarity with PCI, but "we intend to help them," he says. ControlScan will be calling merchants, helping them pick the appropriate questionnaire, and staying on the phone to assist while the merchants fill out their questionnaires. Some TransPay merchants use Internet connections and will need to be scanned by Control Scan, he adds.

Acquirers, through ISOs, are using a carrot-and-stick approach—price incentives or other rewards for early compliance and fines for noncompliance. The closer we get to mandated deadlines, the smaller the carrot will get and the larger the stick will get, Petitti predicts.

### Insurance Gains Traction

While full compliance with PCI standards is proving to be a tough sell to small merchants, insurance against data breaches

has become a big hit. "We offered our merchants a compliance package that includes insurance, and the response has been overwhelming," reports Donna Embry, senior vice president for strategic product development at Payment Alliance International in Louisville, Kentucky. "We expected resistance to something that would add a fee for the merchant to pay. Insurance was optional, and we budgeted for 70 percent acceptance, but we have had 97 percent acceptance. It costs them \$5.95 a month for coverage up to \$250,000, which can cover the cost of fines and reissuing cards. It gives them a comfort level that they're happy to have at that price."

## Even for small ISOs, requiring merchants to comply or lose network access is becoming a fact of life.

—Michael Petitti, Trustwave

While insurance is gaining in popularity, Petitti suggests reading the fine print carefully. Most policies provide protection if a merchant has made a good faith effort to comply and still gets breached. They won't pay merchants that ignore compliance procedures, he says.

### Impractical Principles

Some of the resistance is due to standard-setters insisting on rigid, impractical principles, Martaus argues. Merchants have come to view PCI compliance as a catch 22, he reports. "Rule 6 says that to be compliant you have to develop and maintain secure systems and applications. If you have a breach, you weren't secure, so any breach creates de facto noncompliance and could trigger fines and remediation," he says. "You could think you're compliant. You could have passed all the compliance tests, but if there's a breach, you learn after the fact that you were noncompliant."

"There is a dissonance between the PCI program and actual risk," Abbey agrees.

Even skimming is being defined as a PCI compliance issue now, Martaus complains. "That's old-fashioned fraud, a person in the back room writing down a card number. There's no systematic way you can protect against that, but if it happens, you could be deemed PCI noncompliant."

Litigation has surfaced against the firms that audit and certify compliance for merchants that subsequently are breached, Martaus reports. "If I'm assured by the experts that I'm PCI compliant and that there are no actions I need to take, and then I am breached and defined as PCI noncompliant, the experts should have to answer for that," he says.

The ultimate result of data security concerns is that large retailers adopt end-to-end encryption, not because they are required to but because they will choose this as the most manageable way to secure data, Martaus predicts.

There is near universal agreement that PCI dominates the whole field of merchants complying with card brand rules and regulations. "Data security has monopolized the game," Cohen notes. There still are surcharge violations and excessive chargebacks, but those are routine. Data security is what compliance is all about these days.

Reporting merchant card transaction sales to the IRS is a new compliance issue, but responsibility for that falls on processors, not merchants, Embry explains. And processors will comply without breaking a sweat because they already capture all the data that must be reported starting in 2011. "It will be interesting to see how merchants react when they actually see a copy of what the processor has furnished to the IRS," she says. "Will there be pushback? We'll see." Some cash-heavy merchants could decide to stop accepting cards to escape IRS scrutiny, Cohen suggests. **TT**

---

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