

# State of Compliance REPORT

## The PCI Council's First Six Months See a Rise in Awareness

**C**ompliance was the word on everyone's lips at this year's ETA Annual Meeting and Expo in Las Vegas. From CEOs to merchant-level salespeople, PCI compliance was a hot topic.

In September, the PCI Security Standards Council was formed by the major payment card brands—American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International. Its goal: to provide a transparent forum in which all stakeholders could provide input into the ongoing development, enhancement and dissemination of the Data Security Standard. The purpose is to enhance payment account security by fostering broad adoption of the DSS. So, what has it done so far?

According to members of the executive committee, broad strides have been taken. Seana Pitt, vice president of Merchant Policy & Data Quality for American Express and chair of the executive committee, cites benchmark awareness of the standard throughout the industry.

"In terms of where we are now, given we have just hit our first half-year mark,

it's hard for us to judge, but we are seeing 75 to 85 percent greater awareness and that's half the battle," says Pitt. "That's huge for us. As is the fact that the questions we're getting now are not 'why,' but 'how' can we do this. Compliance has stopped being an issue of having to do it just to make the credit card associations happy. It's now an issue of protecting company brands, financials and keeping customers happy."

helping us revise standards, increase security levels and assure efficiency and implementation of the standard. What we missed pre-council was the industry voice. We've reached out and asked companies to join us at the table. Our current focus is a collective brain trust of the industry."

Pitt boasts that the PCI Council has become a resource to which anyone who has questions on the DSS can go.

**"We are seeing 75 to 85 percent greater awareness and that's half the battle."**

—Seana Pitt, chair, PCI Council executive committee

According to Pitt, the recent TJX breach was a wake-up call for everyone in the bankcard business about the importance of compliance.

"We can help companies on their journey and explain why they have to do it quickly," says Pitt. "We've already done great things. We have 175 participating members, including processors, banks, acquirers and ISOs. They are all

"There is now one place that a merchant can go to ask questions and get one consistent answer across the industry, and that has taken some of the noise out of the system," says Pitt.

Does all this mean that merchants have embraced the council standard and compliance is on the decline? The council is looking at how to collect such data to be an authoritative research

point as well. Pitt believes, though, that few merchants or banks don't understand the urgency.

"As an industry, our biggest challenge really depends on what marketplace you are in," says Pitt. "For instance, some companies need to find out where their data is and get rid of it if they don't need it. Others are challenged with finding out how to stay ahead of the bad guys. You've got to build a better mousetrap if you have a smarter mouse. This is the ongoing evolution of the standard, and as the council is the body that drives this. We are going to need everyone's help to make sure that it's not just the card brands looking at it but everyone adding their experience, their comments and making it very robust without losing sight of implementation of the standard."

### Education Is Essential

Pitt believes education is most important. Toward that end, the council is working on a better outreach program for POS applications for Level III and IV merchants. This particular market segment is proving to be more difficult than any other. In fact, the council is working closely with Visa to adopt its proprietary payment application best-practices technology.

"We realize we need to be more prescriptive with Level III and IV," says Pitt. "We're revamping the self-assessment questionnaire so the average retail merchant or restaurateur can answer it. We need to educate our customer bases as well. And I see it happening. I'm pretty optimistic about the future because the biggest change has been the shift that this is no longer a credit card compliance activity but now a business practice that everyone needs to do to take care of customers."

PCI Council member Brian Buckley, senior vice president of International Risk Management for Visa International, shares Pitt's optimism.

"We are way further ahead than we were six months ago and almost unimaginably further ahead than we were two years ago," says Buckley. "We

have clarified the message of the importance of this issue and we are unanimous in our voice of what the issue is and how it should be addressed. That has resonated in the industry and gotten everyone's attention.

"The council has provided a forum that none of the brands could have achieved independently," he says. "We've created an elaborate landscape of unprecedented access with acquirers, ISOs and banks. Such access allows for blockbuster growth rate of compliance."

Executive committee member Rob Tourt, vice president, Network Services for Discover Financial Services, echoes his fellow members' positive outlook.

"My feeling is that the payment environment is safe, but I also believe that there are things we can do to make it safer," says Tourt. "One compromised event in the press is one too many, but we've made terrific progress. ... We have crystallized the importance of data secu-

ity. We've given our constituents one thing to aim for."

### The Biggest Challenge

Tourt sees the evolution of the standard as being the biggest challenge for the council.

"When I view the standard, I look at it in two-fold terms—effectiveness and efficiency," says Tourt. "Can the standard respond quickly if there is a new threat? We have to constantly be vigilant. When I started my career with Discover, the threat was criminals who figured out how to use re-embossed numbers on cards. Unfortunately, this is a game that constantly evolves. The PCI DSS needs to be a dynamic standard that can respond rapidly to the next threat.

"On the efficiency side, we have to talk to our merchants and discuss what else we need to change in the standard that doesn't diminish it but makes it easier to comply with. We have to

## ADVERTISERS INDEX

### ACH Direct

Page 23  
866-290-5400  
Achdirect.com

### Authorize.Net

Inside Front Cover  
866-437-0491  
authorize.net

### Credit Union 24

Page 4  
877-570-2824  
cu24.com

### Data Systems

Page 18  
843-856-1025  
datasystemscountry.com

### ExaDigm

Page 19  
866-EXA-TEAM  
exadigm.com

### IRN Payment Services

Pages 12-13  
800-366-1388 x 210  
partner-america.com

### ISTS Worldwide, Inc.

Page 37  
510-794-1400  
istsinc.com/retail

### Merchant Management Systems

Page 2  
800-795-6899  
onlinewithmms.com

### National Processing Company

Page 7  
877-300-7757

### npc.net TransFirst

Back Cover  
800-669-7228  
transfirst.com

### TSYS Acquiring Solutions

Inside Back Cover  
480-333-7799  
tsysacquiring.com

### USA ePay

Page 18  
866-USA-EPAY  
usaepay.com

### To Advertise in Transaction Trends CONTACT:

Drew MacFadyen at  
800-394-5157, ext. 37  
dmacfadyen@mceill-group.com

have our eyes open and constantly look to see that it remains effective and stays efficient.”

Tourt believes the PCI Council must continue on the path it started.

“We need to focus on merchants that may be vulnerable to an attack,” Tourt says. “If you are touching a transaction, you can’t store the track data. That’s a very simple but fundamental piece of the puzzle. When you consider the technological complexities of the payment system, and when I look at the progress since the council was formed, there has been a clear clarification of the problem.”

### **New GM**

Hoping to continue that clarity is newly appointed PCI Council General Manager Robert M. Russo. As founder of a number of software and security companies and someone who has held executive management positions in focused security, software and technology organizations, Russo brings years of experience and expertise to the council.

“As the new GM, my biggest plan for 2007 is to get as many of our stakeholders as I can to join us and help craft the standard,” says Russo. “It’s a living organism. A lot of people say it is a moving target, and that’s also true. It has to grow, and we want to make the policy and standard robust and implemental. We want input from all merchants and services providers. Tell us what needs to be done. Help us make the standard better.”

Russo believes that the current PCI DSS is the most progressive, pointed standard out there. He sees it as very prescriptive and informative, likening it to a digital “12 step” program—the first thing to do is admit something is wrong.

“Help us craft our mission,” says Russo. “We need as much help as we can get on this daunting task. There are so many things to look at as far as security, and things change on a daily basis. We are asking for feedback from our participating stakeholders as well as from our Qualified Security Assessors and Approved Scanning Vendors so that we have real-world experience from everyone who has to go through assessments.”

If feedback is high on the council’s list, consulting firm The Strawhecker Group is happy to oblige. TSG Associate Cliff Gray has 17 years of experience in the payment industry, with expertise in technology and integration. He has worked with more than a dozen of the firm’s clients on compliance issues.

### **‘Little to No Gains’**

“In terms of compliance, I honestly believe we’ve made little to no significant gains,” says Gray. “I understand the council’s perspective, but breaches like TJX and Card Systems reiterate just how far we have to go. It’s not fair to look at just the number of merchants who are compliant versus one who is

throughout the transaction, visible only to the account holder and issuer, is critical. Encrypting data is a merchant environment issue, and ISOs and banks will never have complete control over that environment. ISOs and banks must openly force their merchants to be compliant, and the only compliance program with any teeth in it is a program where noncompliance equals nonacceptance.”

Gray says penalty fees are not a deterrent and enforced only if a merchant is breached. He believes acquirers must take the initiative to hire third-party companies to value their merchants.

“If the merchant does not comply within a certain time frame, then it is the responsibility of the banks to deny

**“The only compliance program with any teeth in it is a program where noncompliance equals nonacceptance.”**

—Cliff Gray, The Strawhecker Group

not when that one merchant can have a significant liability, as was the case with TJX and its 40 million cards.”

Gray sees the council positively impacting the industry in that it has removed some of the association bias from when PCI was managed by the associations directly, but not much more.

“We have a long way to go,” says Gray. “The council hasn’t significantly impacted the situation. They need to really broadcast their message. They need to do a tremendous amount of notification and education. ... I truly believe too many merchants don’t realize they are driving without insurance.”

Gray sees two challenges for the PCI Council and the industry in regard to compliance: The issue of Level III and IV merchant IT ignorance, and securing the actual payment credential.

“Apparently payment networks are built around payment credentials that are unencrypted,” says Gray. “Encrypted credentials that remain encrypted

acceptance,” says Gray. “Eventually there will come a time where some critical mass is reached. Today, ISOs don’t want to enforce compliance because it holds the threat of attrition. However, that situation can flip where acquirers don’t offer a full compliant program to their merchants. If they don’t provide a good program with their sponsor banks, then perhaps the merchants won’t come to them at all. Today, merchants may leave if the banks make them comply. Tomorrow, they’ll leave if the banks don’t provide a fully compliant program. We’ve got to put responsibility on the banks. The PCI Code says that’s where it is now. The banks may have the responsibility but they are not doing all that much about it.”

For Gray, the bottom line is that PCI DSS is an underwriting and risk assessment issue until ISOs and banks fully integrate PCI standards into the process. Until then, PCI DSS remains an unfulfilled strategy of the council. **TT**