

# PCI Czar

**The man driving transaction security compliance, Robert Russo, reveals PCI Council positions, ISO education initiatives, and more**

## KEY NOTES

- ▶ The PCI Council will not be considering any list of recognized compensating controls for auditors.
- ▶ ISOs and acquirers will soon be able to access a series of educational webinars they can use to better inform merchants about compliance.
- ▶ Russo believes there's no role for the council in managing a penalty structure. That would force card brands to engage in activities that could violate anti-trust regulations, he maintains.

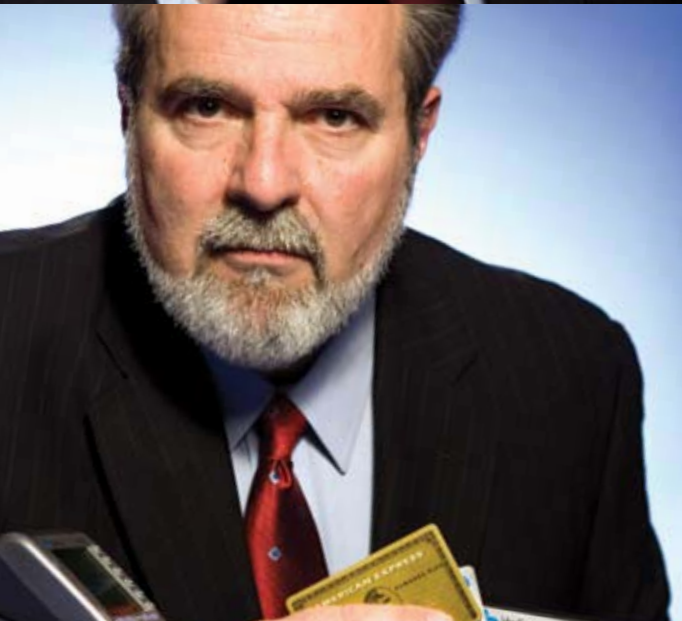
If you think it's tough to convince one merchant to become compliant, try being the person who has to do it for the entire payments industry.

As the first general manager of the PCI Security Standards Council (PCI SSC), it's Robert Russo's job to get stakeholders on the PCI Data Security Standard (PCI DSS) bandwagon. He oversees the PCI Council's training, testing, and certification programs for Qualified Security Assessors (QSAs), Approved Scanning Vendors (ASVs), and related staff, and is the key resource for the certification process. He also coordinates research and analysis regarding PCI DSS, solicits feedback from the vendors and merchants, and steers council member recruitment.

As Russo gets ready to celebrate his first anniversary in this demanding role, *Transaction Trends* asked him to reflect on the past 12 months and his vision for keeping transactions on the straight and narrow.

**Transaction Trends:** What is your perspective on the state of PCI compliance, and how do you expect compliance to evolve in the coming years?

**Robert Russo:** It's been quite a remarkable change in attitude among the players involved in payment card security, especially among the merchant community. When I first joined, I consistently was asked by stakeholders, "Why do I have to do this?" Clearly people were ner-



Photos by Jeffrey Holmes

◀ Robert Russo, General Manager, PCI SSC, says the council is working to bring greater awareness to small merchants, starting with an updated self-assessment questionnaire.

vous about the standards and the effort needed to implement them. But a funny thing happened along this journey. In less than a year, and due to the efforts of the council, card brands, and others all raising the awareness bar, those same stakeholders were asking me just a few months later “OK, how do I do this?” and “How do I do this fast?” In other words, their entire thought process had shifted from one of disbelief and annoyance to one of accepting responsibility for safeguarding their customers’ data.

**Transaction Trends:** One of the most pressing challenges facing the payments industry is to increase PCI awareness and compliance among the small-merchant community, the so-called “tier 4” merchants. What is the council doing to make it easier and less costly for these small merchants to become PCI compliant?

**Russo:** In our first year, we looked to raise awareness and increase adoption of the DSS among the largest merchants by addressing the largest vulnerabilities risks first. As we have seen compliance rise among this group, one of our challenges this year will be to bring greater awareness to smaller merchants. To do that, we will be releasing an updated self-assessment questionnaire (SAQ) for merchants and service providers. The SAQ is an important validation tool primarily used by smaller merchants and service providers to demonstrate compliance to the PCI DSS. This new SAQ is specifically

designed to simplify and streamline the assessment process and aid smaller merchants in their ability to protect payment card data. With the introduction of the updated SAQ, smaller merchants will now have a better understanding of the steps necessary to secure their payment data and comply with the PCI DSS.

**Transaction Trends:** The PCI Council recently assumed management of the PIN Entry Drive (PED) and Payment Application Data Security Standard (PADSS) security requirements formerly managed by the major payment networks. Are there other standards that you believe may be a good fit to bring under the council?

**Russo:** The addition of the PED and standards under the management of the council were logical moves that reinforced and expanded our commitment to securing the payment process globally. In the future, we will continue to consider any

measures that similarly remove conflicting requirements, simplify the testing process, and maintain consistent security measures to improve the overall security of payment transactions.

**Transaction Trends:** Earlier this year, the council elected a Board of Advisors to provide strategic and technical guidance on the standard. Can you tell us a little more about the role the members serve and how they have effected change?

**Russo:** Our Board of Advisors continues to provide strategic and technical guidance to the council. Members reflect the varied perspectives of different global stakeholders and offer input that is critical to the ongoing enhancement of the security standards we manage. For example, they were instrumental in the development of our focus areas and workshops at our community meeting. Their real-world experience helped to establish the agenda and frame the discussion for all of our stakeholders.

# Inside the Council

The PCI Security Standards Council was founded in 2006 by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International. Its mission is to enhance payment security by fostering broad adoption of the PCI Security Standard.

The organization consists of an Executive Committee, a global Advisory Board that provides strategic and technical guidance, a Management Committee that runs business operations, a Technical Working Group, which "evolves" the PCI Data Security Standard, and a Marketing Working Group for ongoing marketing activities. The general manager oversees day-to-day operations.

Members must be "multi-national acceptance marks" with an ongoing commitment to PCI Security Standards. Other payment industry stakeholders, such as merchants, banks, processors, and point-of-sale (POS) vendors, can support the council as Participating Organizations.

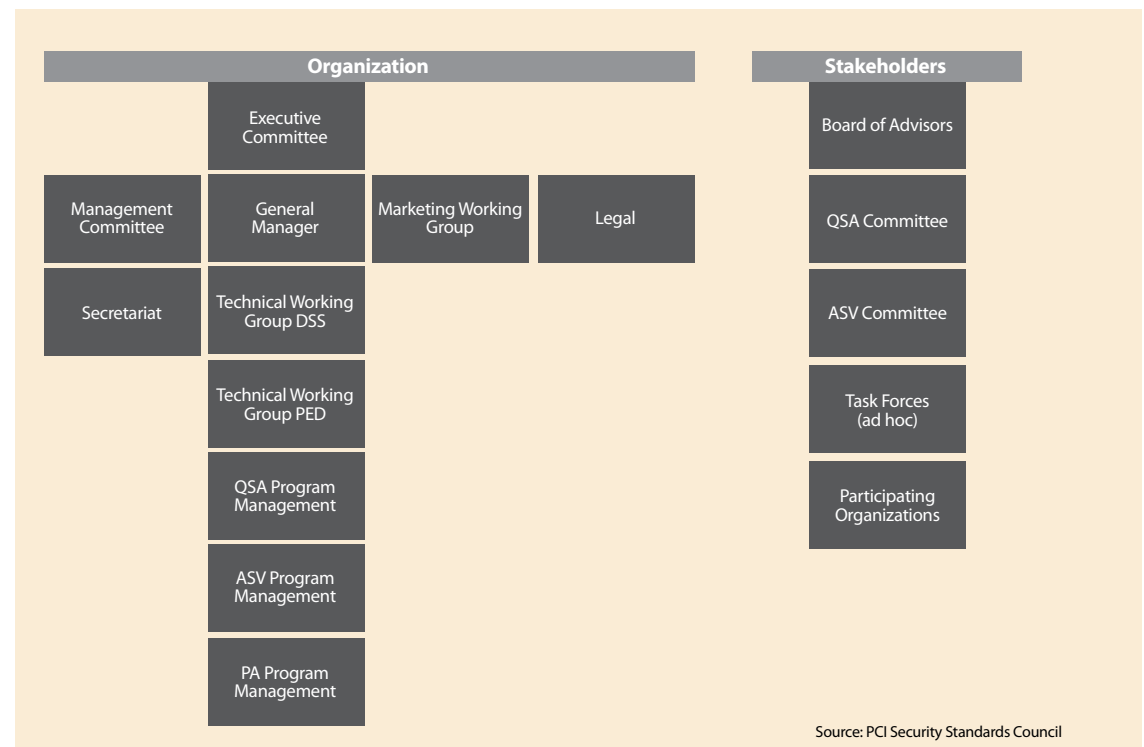
The council was initially funded by contributions from the participating payment brands. In

the long term, it will be funded through ongoing business operations, including QSA and ASV approval programs. Its other activities include:

- developing and managing the PCI Data Security Standard, including maintenance,

- clarification, and revisions of the Standard;
- publishing and distributing the PCI Data Security Standard, including errata and addenda, and all related documents associated with QSA and ASV policies and procedures; and

- providing an open forum where all key stakeholders can provide input into the ongoing development of other payment security standards and business practices.



Source: PCI Security Standards Council

**Transaction Trends:** A recent study conducted by Air-Defence (a wireless security products maker) found that about 25 percent of the more than 4,000 retail stores surveyed were exchanging data with no encryption, and another 25 percent were using an outdated encryption method that can be easily compromised. How big of an issue is it to secure payment data being transmitted through wireless networks, and is this covered by the PCI Data Security Standard?

**Russo:** Wireless security is an important aspect of any thorough security posture. In fact, wireless security was one of the key areas of discussion at our global community meeting held in Toronto last September. The DSS has very specific security requirements (DSS requirement 4.1.1) for wireless networks transmitting cardholder data, and meeting this requirement is essential for PCI compliance. We are working closely with retailers to identify and mitigate issues related to wireless technologies in payment environments and evolve the security of this technology now and in the future.

**Transaction Trends:** While the council is responsible for managing the PCI standards, the individual card networks remain responsible for investigations and enforcement actions. Do you believe there is a role for the council to manage a framework for standard or minimum penalties to ensure that violators are treated equitably?

**Russo:** No. Moving in such a direction would mean the card brands are engaging in activities that could fall under anti-trust regulations. The system works well with multiple players having multiple enforcement capabilities.

**Transaction Trends:** One of the big changes in the last major update to the PCI standard was the introduction of “compensating controls” that provided businesses with some flexibility to achieve compliance. Because an auditor must determine whether an implemented control is adequate, some have observed a degree of subjectivity as to what is determined compliant. What’s your take on compensating controls, and do you expect the PCI SSC to issue any “safe harbor” examples?

**Russo:** The council wants to provide all reasonable avenues for compliance under the standard. So the need for compensating controls provides that flexibility. This year, the council will undertake a comprehensive quality assurance program for all of its assessors. We believe this is the best and most prudent course of action to ensure—as much as humanly possible—consistency among proposed compensating controls. Beyond that, I don’t think the council will issue any such “safe harbor” provisions.

**Transaction Trends:** Do you foresee a convergence of payment security requirements for merchants beyond the traditional payment card networks, for example Automatic Check Handling rules and regulations?

**“Both the council and the card payment brands have a tremendous wealth of information on their Web sites that ISOs and acquirers can use to better inform their merchants about PCI DSS and the path to compliance. In fact, the council will be starting a series of educational webinars for stakeholders during 2008.”**

— Russo

**Russo:** We continue to see organizations wanting to utilize the PCI DSS as the basis for security beyond payment card processing, and organizations like the National Automated Clearing House Association are looking at implementing the PCI DSS into their framework. So I would have to say “yes,” but we are not necessarily promoting that fact.

**Transaction Trends:** Because PCI is an international standard, what is the level of awareness and compliance outside of North America and what are some of the biggest challenges for global adoption?

**Russo:** Similar to the United States, international companies are fundamentally in agreement when it comes to data security. Regardless of their location, companies know that protecting their customers’ card data is the right thing to do and an essential part of doing business. To raise awareness and promote the adoption of the DSS internationally in the next year, we will continue to increase participation outside of North America; grow QSA and ASV availability in underserved areas; provide core PCI SSC resources in additional languages; and implement proactive press outreach in target non-North American markets.

**Transaction Trends:** What are some of the ways ISOs and merchant acquirers can help promote greater awareness and compliance among their merchants?

**Russo:** Education is the key. Both the council and the card payment brands have a tremendous wealth of information on their Web sites that ISOs and acquirers can use to better inform their merchants about PCI DSS and the path to compliance. In fact, the council will be starting a series of educational webinars for stakeholders during 2008. We will continue to produce other materials and opportunities, including merchant training on DSS, because it’s central to the PCI Council’s mission. **TT**