



July 27, 2009 • Issue 09:07:02

Allied vendors speak

Data security remains one of the most visible and controversial issues affecting the payments space, underscored by a number of high-profile data breaches in recent years. Such events have helped spur debate about the viability of the **Payment Card Industry (PCI) Data Security Standard (DSS)** - regarding the regulations themselves and their implementation - particularly with merchants, for whom PCI compliance has proven especially challenging.

An announcement at the **Electronic Transactions Association** Annual Meeting & Expo in April 2009 by the founders of the **Secure POS Vendor Alliance** marked the organization's official inception, setting the stage for a more pointed debate on issues relating to data security. The SPVA's general purpose is to help address the voluminous, and often complex, concerns of those in the industry - merchants, acquirers, issuers, et cetera - for whom data security is a central concern.

The Green Sheet spoke with the SPVA's three founding members: Paul Rasori, Senior Vice President, Global Marketing for VeriFone and SPVA Secretary/Treasurer; Christophe Dolique, Executive Vice President, Global Marketing and Transaction Services for Ingenico and SPVA Chairman; and TK Cheung, Vice President, Global Quality and Security for Hypercom Corp., and SPVA Vice Chairman and Chief Technology Officer.

The following is excerpted from the conversation:

The Green Sheet: What is the aim of the SPVA?

Paul Rasori: First and foremost the goal of the alliance is to better align point of sale vendors with the various [PCI] security standards in an attempt to try to clarify what's going on out there in the marketplace.

We are soliciting membership from essentially any point of sale vendor that does business in the space and any other company that interacts with the payments system, including acquirers, banks, retailers and so forth.

The idea is to develop a set of interpretations of the existing standards, so when you select vendor A versus vendor B, when they've gone through what we call an SPVA approval process, it's much clearer what you're getting in return. That's just one of the areas. Another area is we see some gaps in the existing security standards, and we've set up working groups to try to address those gaps to try to raise the level of security overall.

One of the key focuses of the SPVA is to work to develop standards around things like end-to-end encryption of credit and debit card information. Another area is standardizing the payment device life cycle from the point of development, manufacturing and deployment, to the ongoing operation of that device while it's in service and all the way up through the secure destruction of these devices once they're [out of service].

GS: What do you mean by "standardizing the life cycle" of payment devices?

PR: Today there's no standard whatsoever that governs the deployment of a payment device in terms of the life cycle of that device. You can go on to eBay today and purchase payment devices, but who's to say there's not residual consumer information on those devices you're purchasing? Who's to say criminals aren't using those devices to be used fraudulently?

So there are no regulations in terms of where these devices end up and how they're managed over the course of their life cycle.

GS: Paul Rasori mentioned the "SPVA approval process" in reference to helping merchants select a security vendor. What does the process involve, and where is it used?

TK Cheung: SPVA is committed to accelerating wide-spread adoption of enhanced security guidelines. Merchants that choose SPVA-approved solutions will be assured they are providing consumers with the highest level of security currently possible and protection against future threats. They will be able to more easily comply with current industry mandates such as PCI, and compliance with individual card brand rules. This will reduce their risks and ensure their investments against future changes to security requirements.

GS: You say part of your aim is to help "interpret" the PCI DSS for merchants and other industry players operating under the regulations. What makes them so difficult to understand and why do they require interpretation?

TKC: The overall complexity of electronic payments has increased and gone global, bringing a new set of security and regulatory challenges and making life more demanding for merchants and acquirers to implement and manage secured and cost-effective payment solutions.

The multiplicity of rules together with the fact that various countries have their own rules makes it very difficult for all stakeholders to have a common understanding of the whole payment security value chain. SPVA will develop a common understanding of the various security requirements and standards and provide easy-to-understand guidelines to ensure security against threats and attacks.

Christophe Dolique: One example is contactless solutions. There are different contactless solutions, and our point is how can contactless work together in the same terminal and provide the same level of security? It's an example of a challenge we need to address.

GS: How will you address the needs of merchants who can't afford to upgrade an outmoded security system?

TKC: Affordability is balanced against the risk of fraud. More exposure will dictate the shift toward newer and more effective methods of security, and this is not limited to merchants. The cost of conducting business and the ability to accept electronic payments means that transaction acquirers, issuers and merchants and other key stakeholders in the payment value chain must protect critical customer data.

The cost of not doing so will be far greater due to the likelihood of lost business as a result of any breaches.

GS: Are things being done in other countries to secure contactless payments that we might do well to emulate in the United States?

PR: Right now it's up to each individual card brand to define how each of their contactless programs work, so one card brand may employ a certain security where another one wouldn't.

And the way it works today is each vendor, such as VeriFone or Ingenico, must implement each individual program separately. So even within the same terminal you may have a more secure way to take card brand A than card brand B, and that's because we follow different rules on how that is accepted.

Christophe and I were just talking about reaching out to the EMVCo [the Europay, MasterCard and Visa International standards body], which today is the global standard for chip card acceptance, and they've actually done a good job of creating that standardization, so it's pretty standard across the world how a typical smart card is accepted.

And our goal is to reach out to them and work with them toward a similar standard for contactless.

GS: What are you doing to attract members to the organization?

PR: Each of us is calling directly with a lot of the industry contacts we have. We've been speaking at various forums around the world - I know we've spoken at several in the U.K. and France and the United States. Each founding member is individually holding discussions, webinars and/or meetings with our top customers.

GS: What size membership do you foresee for the organization?

CD: Between 20 and 50 members at least. We have a chance to be quite active in the creation of the new structure - like the way new payment rules are going to be defined. And I think it's important regarding this fact that major players in this industry be contributors to this creation.

GS: What are some of the benefits associated with SPVA membership?

TKC: Members can, through their participation and leadership on technical working groups, help shape future security guidelines and acquire first-hand knowledge of current security threats and ways to mitigate them.

GS: How is your organization structured?

CD: We have an organization with five board members. There's three founders: VeriFone, Ingenico, and Hypercom, and two seats left for people acting in the POS business. Two of the members are elected, and the other three members are permanent. But this alliance is open to any member from the payments ecosystem.

GS: Where specifically did the idea come from to create the SPVA?

PR: I think it came about in 2008 when the three [founding] CEOs were together at the card tradeshow held in Paris every November. I think they just got into a general conversation about what some of the issues in the industry are and just planted the seed of the idea: Is there a way for us to better influence what's going on?

I think the realization was that in general, vendors in our category have always been followers in this industry as it relates to a lot of these standards and haven't been proactive enough in providing the perspective of the companies that implement these solutions. We began more formal discussions probably in the January [2009] time frame and launched it in April.

GS: Are you working directly with the PCI Security Standards Council to help develop your game plan and provide them with feedback?

PR: Yes, we've had a lot of interaction so far. Certain members of our organization participate in their [special interest groups], but one area we will be focusing on with them is they've recently hired an outside consultant to look at the whole end-to-end encryption issue, so we've been in contact with them and participating with them on that particular topic - which is probably the one that's most relevant.

In addition, we'll be reaching out to them as we develop our interpretations of the existing standards around PCI, to make sure it aligns with their goals.

Because ultimately the number one priority of our organization is not to replace the standards but to better implement the standards.

So it's not competitive, if you will, with an organization like the [PCI SSC]; we really look at it as complementary, and so far the feedback from the PCI Council - as well as the members that represent the card brand that runs the council - is I would say cautiously optimistic. They welcome a unified voice of the POS community because it helps them implement what they want to implement faster.

GS: Do you have confidence in the PCI DSS? Do you think PCI SSC members and industry leaders understand the security needs and concerns of the average merchant?

TKC: We have every confidence in the PCI DSS and the base standard guidelines that the industry follows. Council members are elected from a broad spectrum of companies to ensure the widest possible representation of acquirers, processors, merchants and those related to electronic commerce. With the SPVA's global reach, the three founding members

have the ability to analyze global security threats and increase awareness to meet and exceed the base standard guidelines in the most effective manner by working alongside the PCI DSS and reinforcing the message.

Notice to readers: These are archived articles. Contact names or information may be out of date. We regret any inconvenience.