PCI Community Meeting Recap

It's no secret that Shift4 and the PCI Council don't always see eye-to-eye. We may not like every standard they issue, but we do recognize the efforts they have made to standardize credit card security best practices around the world. We also understand that the QSAs they train are the people who ultimately decide whether our merchant customers get the simplified PCI experience that we promise in our marketing materials.

That was the real motivation behind our sponsorship of the PCI SSC North American Community Meeting in Las Vegas (our hometown) last month. From hosting a packed-to-capacity welcome reception at Las Vegas' famous House of Blues, to introducing our brand new (and enormous) tradeshow booth, it was a busy and exciting week for Shift4 as we embraced our role as Diamond Sponsor.

Perhaps the best moment of all, though, was when we invited 160 of the industry's top minds (including QSAs, ISAs, and other industry experts) to the exclusive Foundation Room atop Mandalay Bay for a reception we called "The Main Event." We billed the event as a meeting of the minds and an opportunity for us to come together and hash out solutions to the industry's most vexing problems – and that's exactly what we did.

We talked about everything from the training of QSAs to the value of our TrueTokenization® in comparison to the simplified (bastardized, as we call them) solutions that our competitors offer. Here are a few of the highlights:

P2PE at the Service Provider Level

Merchants look at P2PE as the ultimate scope-reduction solution. The existing hardware/hardware and hardware/hybrid specs allow them to reduce scope only from their endpoints, leaving their HQ or datacenter fully in scope of PCI assessments. If merchants could outsource decryption and key management to their service provider (that already is – and will always be – fully in scope for PCI DSS), they could vastly reduce their breach profile and their scope.

PCI announced they will release software-P2PE specs early next year, and we certainly hope they follow through so that the customers already using our P2PE solution can finally see the promised scope-reduction benefits of the SAQ P2PE-HW.

QSA Training and Standardization

We often compare QSAs to snowflakes, joking that no two are the same when it comes to assessments. One QSA in attendance seemed to agree with us and raised questions about QSA training. Is it too easy to become a QSA? Why do they often assess the same company so differently?

Ultimately, the value of a QSA comes down to their ability to look strategically at an issue. Those who simply check compliance boxes without giving a second thought as to the actual security of the solutions at play do very little good for merchants. In fact, one ISA in attendance admitted that he wished his QSA would be harder on them during their annual assessment, but said he knew the QSA firm was afraid to lose their business and therefore encouraged the QSA to "make sure everything went well."

We need QSAs who not only understand the requirements, but who also have the ability to see how those requirements can be adapted to cover new solutions and new technologies.

The Scoping of Tokenization – and Its Definition

PCI tells us all to consult our QSA to determine the scope of our tokens. Why? Because not all tokens are created equal. We should know — after all, it was Shift4 that introduced the term tokenization back in 2005 and who cried at what we call the "Great Bastardization of Tokenization" in 2011 when PCI decided that hashing or encryption schemes, format preserved or otherwise, and a host of other less-than-adequate solutions would pass as tokens.

While they're not willing to shrink back their definition of tokenization, PCI Council executives did confirm to us during the Community Meeting that tokens that hold a one-to-one relationship with the original PAN will not allow for scope reduction. Likewise, mathematically derived, format preserving, 16-digit numeric tokens are not secure enough on their own to warrant a reduction in scope. Fortunately for us, Shift4's organically generated, random, alphanumeric TrueTokenization® meets all of PCI's requirements for scope reduction.

The Merchant-is-always-liable Approach to PCI Enforcement

A comment we often hear from our merchant customers: "If I'm breached, it doesn't matter how much I've forked out on PCI, I'm still going to be found liable." Merchants and processors have passed PCI assessments while their systems were actively being compromised; they were compliant then, but suddenly were deemed noncompliant once the problem came to light. What is the purpose of PCI compliance if it is revoked the moment you need it most? We asked an entire room full of assessors and not one could name a merchant who had been protected by their PCI compliance.

If, despite their best efforts (and vast expense) no victim of a data breach has ever been found to be PCI compliant, what is the motivation for merchants to seek compliance?

At the meeting we brainstormed an idea of having a PCI grading scale that would actually provide an incentive for merchants to strive for and maintain adequate CHD security. QSAs would provide a letter grade to merchants based on their breach profile and taking into account any demerits for risky behavior. Almost like a health inspector, we proposed that QSAs could make these assessments through annual inspections and/or surprise visits. Best of all, if a merchant were breached, the PCI grade would come into play in assessing fines. Those with an "A" grade might not receive any fines, whereas a "C" grade and lower might have a discount rate penalty in addition to fines.

As you can see, we covered a number of key topics and also had plenty of laughs (and a few rants). We relayed many of our attendees' concerns and proposed solutions to the PCI Council. Now we have to wait and see how these get put into action in the next round of QSA training and subsequent assessments. Hopefully our investment pays off!

About Shift4

Shift4 is dedicated to maintaining the trust of more than 24,000 merchants who rely on their DOLLARS ON THE NET® payment gateway to process upwards of half a billion credit, debit, and gift card transactions each year. Shift4's commitment to innovation keeps them at the forefront of emerging technologies including P2PE, mobile, EMV, and tokenization. Shift4 helps businesses secure the lowest possible payment processing rates and protect their brands by securing their customers' card data.

Shift4®
Secure Payment Processing
1491 Center Crossing Road, Las Vegas, NV 89144
702.597.2480 | 800.265.5795
www.shift4.com | info@shift4.com