Evan Schuman's
StorefrontBacktalk
Techniques, Tools and Tirades about Retail Technology and E-Commerce

Mobile POS Moves Forward, With MasterCard's Blessing

Written by Walter Conway
May 30th, 2012

A 403 Labs QSA, PCI Columnist Walt Conway has worked in payments and technology for more than 30 years, 10 of them with Visa.

I have just seen the future of mobile point of sale (MPOS), and I think those ubiquitous plug-in card-reading dongles may be winning. It doesn't matter that these MPOS approaches pose risks for cardholder data, that the payment applications are not PA-DSS validated or that they are not part of a point-to-point encryption (P2PE) solution as recommended by the PCI Council. What does matter is that the card brands have embraced them as the MPOS approach for merchants of all sizes, even while recognizing that it may be difficult for these same retailers to achieve PCI compliance.

MasterCard on May 23 released formal guidance giving retailers a roadmap to implement MPOS using smartphones, tablets and other devices equipped with a "card reader accessory." The problem? The recommended best practices may not be PCI compliant and they conflict with MasterCard's own rules, as the card brand acknowledges.

This situation poses the question, "What is a retailer to do?" I don't have any simple answers. But MasterCard's recommendations seem to point a way forward, while simultaneously acknowledging the business risks and conflicts with PCI.

The guidance is targeted at very small merchants "that previously operated on a cash- and invoice-only basis." MasterCard even invented a new category for small merchants to accommodate the growing needs of these MPOS retailers.

The document also targets larger retailers "adopting MPOS solutions and integrating them into their current point —of-sale environment to enhance the retail and payment experience." That means the target audience includes just about every retailer.

MasterCard's "Best Practices for Mobile POS Acceptance" tell merchants how they can process payment cards today using their smartphones, tablets or PDAs combined with an attached "card reader accessory" or dongle. MasterCard cites the growing shipments of MPOS solutions and the resulting increase in payment card acceptance at traditional cash- and check-only merchants as the driving force.

Not wanting to be left behind any competitors, maybe MasterCard felt the prudent course was to get in front of the MPOS parade by issuing its own set of retailer best practices. After all, Visa clearly expressed its own support for MPOS when that card brand announced in April it had actually invested in Square, a leading dongle vendor.

The best practices document recognizes that an MPOS solution provider may be a "Payment Facilitator." A payment facilitator has a merchant agreement, and it essentially resells card processing to its "sub-merchants," e.g., small merchants who do not need their own acquiring relationship. This puts payment facilitators somewhere between an independent sales organization and a PCI service provider. Payment facilitators must register with

MasterCard and follow the program rules, including screening their sub-merchants and guaranteeing that none of them processes more than $100,000 in card transactions (presumably annually, but no time period is specified).

Memo to all potential payment facilitators: Make sure to check the MasterCard program rules. Check, too, with your QSA. It may be that your own PCI assessment will need to include a sample of your sub-merchants. They seem to be in your PCI scope, because you are the merchant. Then again, it may be that the card brands will lump payment facilitators with service providers. But if that is the case, why the separate program?The most relevant parts of the document for retailers are on pages five and six. Here MasterCard makes it clear it is talking specifically about mobile devices with a card reader (or dongle) "attached to the audio port, USB port or proprietary connector," and the merchant uses a payment application installed on its smartphone or tablet to process the transaction. The card brand excludes contactless solutions where customers use their own device as a replacement for the physical payment card.

Things start to get interesting because, as MasterCard puts it, merchants face a "unique challenge." Specifically, MasterCard mandates that merchants use only PA-DSS validated payment applications listed by the PCI Council. But, as the document notes, "the PCI SSC is not certifying MPOS payment applications that reside on multi-purpose consumer mobile devices until further guidance is developed to ensure the security of cardholder data within the mobile device." Get it? Retailers must use PA-DSS validated applications, but there are no PA-DSS validated mobile payment applications.

To me, this definitely qualifies as a unique challenge—or maybe even an insurmountable opportunity. What's the answer? MasterCard appears to be saying merchants should follow its (meaning MasterCard's) prescribed best practices. But as a QSA I recommend full PCI compliance at all times.

MasterCard tells MPOS solution providers that they "should" (note: not "must") develop their code securely, update the application and have policies in place when their sub-merchants lose their MPOS device. The card brand tells merchants that they "should" (again, note: not "must") talk to the solution providers about security.

That is about all solution providers need to do, and the "unique challenge" posed by the lack of PA-DSS validated mobile payment applications goes away. Again, as a QSA I have to reinforce the importance of using only PA-DSS validated applications installed and maintained according to the vendor's PA-DSS Implementation Guide.

MasterCard recognizes another "unique challenge" a bit further on in the document. It notes that the open architecture of mobile devices and their susceptibility to malware can lead to the loss of unencrypted cardholder data. Because of these "limitations with the security features of mobile devices, merchants who use MPOS solutions will find it challenging to comply with the requirements of the PCI DSS."

Did I just miss something, or did a major card brand just give MPOS merchants and sub-merchants a pass on PCI compliance? Or, is MasterCard taking a risk-adjusted approach to compliance? I do not think the card brand is doing either, but it could be confusing. MasterCard notes at the very beginning of the document that none of the best practices supersedes any of its rules. Still, the recommendations offered do not seem to include an easy path to PCI compliance.MasterCard's guidance leaves merchants on their own to ensure they implement a secure solution. It seems a bit unfair to ask a plumber, farmstand vendor, food truck operator or taxi driver to assess the security of a complicated mobile payment application. All they want to do is sell stuff. And I have no idea how they are to "consult their MPOS solution provider," especially if they bought the dongle online or from their local office supply store or megamart.

As far as I can tell, the only path to a PCI-compliant MPOS solution is the PCI Council's P2PE approach where the smartphone or tablet never sees or stores clear-text cardholder data. The Council described it in its MPOS guidance issued earlier this month, before MasterCard's guidance came out. The Council cites the "new risks to the security of cardholder data" and directs merchants to a P2PE solution as the best (only?) way to achieve a PCI-compliant MPOS solution.

The difficulty is that both retailers and MasterCard recognize there won't be any P2PE approved solutions for

months, and the mobile space is moving rapidly today. Retailers do not want to wait. Not willing to be left out of a growing market (see page 10 for instructions on displaying the brand's acceptance mark on the device's screen), MasterCard has recognized the inevitable and offered a reasonable (risk adjusted?) set of best practices to guide solution providers and merchants alike. As a QSA, though, I would have been happier if there were less "should" and more "must" in MasterCard's recommendations.

Naturally, there are a few questions.

- Will the recommendations (the "shoulds") ever become requirements ("musts")?
- Will MasterCard's best practices change to reflect or even require P2PE MPOS solutions when they become widely available, possibly in just a few months?
- Will the other card brands adopt the payment facilitator and sub-merchant model?
- How happy will acquirers and processors be that payment facilitators have this sub-merchant market segment to themselves, without requiring PCI compliance?
- What happens to the payment facilitator when its first sub-merchant is breached?
- Should payment facilitators be subject to additional PCI-compliance requirements, as service providers are today?
- Once a sub-merchant hits the $100,000 transaction threshold, will an acquirer let it continue to use its non-validated mobile payment application?

None of us knows the answers, but I'd like to hear what you think. Will this set of best practices change your mobile POS plans? I'd like to hear your thoughts. Either leave a comment or E-mail me.