

[FEATURE]

Coming

Although new products will make customer data transfer safer, retailers may be slow to jump on board

By Kim Fernandez

KEY NOTES

- ▶ While cell phone payment systems are intriguing and may well be the wave of the future, critical security issues must be resolved before merchants and consumers accept them.
- ▶ Emerging NFC technologies can help keep consumers' information out of the hands of crooks, but new versions of NFC software would require some kind of authentication before payment would be accepted.
- ▶ ISOs shouldn't expect total buy-in from merchants who may not be willing to pay more to accept payments using the new technologies.

Attractions in Technology

From encrypted card readers providing card and host authentication at the point of sale, to payments software that also generates personalized consumer rewards and coupons, new technologies coming down the pike will, once again, change the way merchants accept credit card payments. This time, the push is to help protect everyone involved from the devastating effects of data theft and fraud—if merchants spring for the upgrades.

“The whole entire industry at this point is based on security,” says David Talach of VeriFone in Rocklin, California. “We see that as the number one area of focus, and see emerging technology to keep an eye on security.”

Others agree, saying that consumers are fed up with the fraud that can follow when they use credit cards to shop using existing methods, and credit card companies are pushing hard to avoid the costs related to recovering cardholders’ money and prosecuting those who commit fraud, if they can even be caught.

“I think you’re going to see a lot more [technology to boost security] because of the breaches that happened last year and this year,” says Franck Fatras of AdvanceMe Inc. in Kennesaw, Georgia. “The Heartland breach was a big wake-up call.”

Meeting the Minimum

New hardware and software currently under development focus almost exclusively on keeping credit card and personal information locked down, either by keeping such data secret to anyone but the cardholder and issuing bank, or by encrypting data every possible moment,

behind electronic walls that would be nearly impossible to topple.

Further, technology developers are leaning toward far exceeding security measures passed by the PCI Security Standards Council because of breaches like Heartland’s, which was hacked into despite being compliant with PCI standards.

“PCI is the minimum, but it’s definitely not where you should be,” says Fatras. “Security is always going to be a concern, especially in an economic downturn. More people may be tempted to do things that might not be good in times like these. Security has definitely been a focus; it’s definitely what keeps us up at night here.”

One development that may result is the ability to charge merchandise to credit cards without actually producing the card at checkout, or even having it on your person.

“There are things that are going to supplement and, in some cases, replace the plastic credit cards people carry,” says ETA’s Tom Goldsmith. “People are going to be using their cell phones to make payments, so when the check comes at the end of your meal, you’ll punch in some numbers and pay for it. It’ll show up at the register without your having to hand

your credit card to a waiter, who’s going to walk away without you knowing where he’s going or what he’s doing with it.”

Other experts foresee a similar future, with programs on cell phones that enable people to pay for merchandise, or keyfobs with the same information that are waved at registers or even accessed merely by being nearby at checkout.

“At some point, everyone is going to have a phone that has this capability or a keyfob or keychain that has this capability,” Talach says. “It’s not a matter of ‘if’ anymore. It’s time to get on with things and think about ‘when.’ There are some rumblings that handset manufacturers will issue some phones with this capability in 2011. These aren’t just trials and betas—they’ll have new phones with attractive functionality and NFC capability.”

Similar technologies are already in use overseas, says Goldsmith. “In Europe, we see a lot of use of pay-at-the-table technology,” he says. “The server brings a wireless device to your table and you swipe your card, similar to the way we do at the grocery store here. The card never leaves your hand, and a wireless transmitter sends the data back to the main terminal.”

While cell phone payment systems are intriguing and may well be the wave of the future, critical security issues need to be resolved before merchants and consumers will accept them.

“Typically, right now if you swipe your credit card, there’s an interchange fee that’s a percent of your transaction,” Goldsmith explains. “That’s divided up from the people who process the payment to the bank that issued the card—everybody gets a slice. If you’re using a cell phone, the question emerges as to whether the cell phone companies are going to let some-



PCI COMPLIANCE? NO PROBLEM.

Simplify PCI

Wondering how to help your merchants become PCI compliant and keep them happy? SecurityMetrics can help. As a leader in PCI-DSS we handle more than 100,000 merchant PCI calls every month. Our Simple approach works.

Call today to receive a free PCI consultation for your business. 801-724-9600

www.securitymetrics.com

securityMETRICS®

body else make the profit on that transaction, or insist it's part of their infrastructure and that they get the fee."

Increased Security

"I see a longer-term trend with increasing the number of POS terminals and being really bullish on NFC and phones," Talach says. "We're positioning ourselves to have a product roadmap and a line of products that will fully take advantage of these new handsets in 2011."

"We're seeing a resurgence of the gateway," he continues. "It's one of these technologies that were initially developed to help aid the first wireless products back in the day. ISOs are becoming increasingly savvy, and we're using products and giving a level of support to merchants who want increasing control of their businesses. So we'll route some merchants' phone transactions through a gateway. It's about what can we provide them to let them differentiate themselves and help mitigate risk."

AdvanceMe has a long-standing policy of using a different vendor for each of its payment needs, and Fatras sees more companies following that trend to help boost security. "We've never had the same company come in twice," Fatras says. "We go with different vendors every year. It's a broader scope of what's out there and how people are approaching it. The security rules have stayed the same, but people are a lot more conscious of it."

Companies are realizing they have to stay one step ahead to guard their data. "You're never going to be 100 percent secure—it's impossible," Fatras adds. "You have to be prepared and as secure as you can be, but if you say you're 100 percent unhackable, you're dreaming."

Emerging NFC technologies are another way to keep consumers' information out of the hands of fraudsters, says Goldsmith. But new versions of NFC software would require some kind of authentication before payment would be accepted.

"You have to have the right terminals, and then you can't read the card until the cardholder gives permission," he says.

"Right now, there's very little authentication involved. If I get your credit card for five minutes, I can tap into the terminal. It's a security issue that people are working very hard to overcome and protect against."

In the not-too-distant future, merchants will likely have terminals to accept PayPal payments during in-person transactions, again, keeping credit cards tucked safely inside consumers' wallets, he adds.



Experts have predicted the advent of credit card readers connected to personal computers to further shore up security.

"Things are moving in a big way to get retailers to accept PayPal," Goldsmith says, pointing to consumers' comfort with the payment system, which keeps account information hidden from the seller. "The customer will have a PayPal number and the seller will have a PayPal terminal. You type information into the terminal and go through the PayPal system. People are looking for some kind of variation on that."

Retailers' Perspectives

On the other side, retailers' spokespeople say that while these new technologies are wonderful, ISOs shouldn't expect total buy-in from merchants. Many simply can't afford to install new terminals to accept cell phone or keyfob payments.

"Retailers are not particularly interested in developing and adopting new technology, especially if it's going to cost

them even more to accept [payments] with the new technology," says Mallory Duncan, with National Retail Federation in Washington, D.C.

While big-box stores may be able to adopt new machines and software packages, smaller retailers will likely be left behind, agrees Nancy Thomas, spokesperson for the Retail Merchants Association in Richmond, Virginia. "Obviously, there's a cost related to any upgrade in processing," she says. "Just being compliant is costly, and there's a sector of retailers really doing the bare minimum because of those costs."

Moreover, Thomas fears that with more sophisticated technology comes the chance for increased processing fees because the devices make it easier for consumers to use credit more often. "I don't see [smaller retailers] using keyfobs and that sort of thing, even though it's good for the consumer," she says. "The POS terminal has to be upgraded, and that's probably nearly impossible for small- and medium-sized mom-and-pop businesses."

But experts on the processing side say that consumers may demand the newer technologies to secure their information. "The older generation has always been nervous with credit cards," says Fatras. "The new generations have been a little bit more lax, but they're also more tech savvy."

Some experts have even predicted the advent of credit card readers connected to personal computers as a way to further shore up security. But Fatras says most consumers won't want the inconvenience and expense of having one at home. They may, however, embrace biometric security measures and readers that don't require them to produce their plastic cards.

One thing's for sure: Consumers will continue to demand better security, and stores risk losing sales unless they find a way to accept transactions without transferring account numbers or passing a credit card through cashiers' hands. **TT**

Kim Fernandez is a contributing writer for Transaction Trends. Reach her at kim@kimfernandez.com.