DISPENSING LOYALTY: REFILLABLE MUG PROGRAMS WORK

NACS®
nacsonline.com
THE ASSOCIATION FOR CONVENIENCE & FUEL RETAILING
MAY 2015

THE C-STORE OMNICHANNEL OPPORTUNITY

SAFETY IN NUMBERS

As tokenization takes hold, the race to establish industry standards begins.


A TOKEN
GESTURE

As tokenization takes hold as a means for protecting personal data, the race to establish industry standards is underway.

Jerry Soverinsky

Lost among consumers during the September 9, 2014, Apple media event that introduced the Apple Watch and large format iPhones was the introduction of a new mobile payment system, Apple Pay.

It's hard to fault consumers for failing to flood social media with plaudits of the Apple Pay announcement. Far less sexy than the toaster oven-sized iPhone 6 Plus, Apple Pay was a relatively late entrant into the mobile payments landscape, following on the heels of a long line of mobile payment initiatives, including Google Wallet and Softcard (formerly Isis).

While uninteresting to those crooning over a wearable device that displays — imagine! — the time of day, Apple Pay is a considerable step forward in protecting personal data during a payments transaction. And it couldn't have come at a better time.

The past few years have been unsparing to some of the world's largest firms and brands and their customers, as Albertsons, SuperValu, Nieman Marcus, Target, The Home Depot, Kmart, Sony and JP Morgan Chase suffered data breaches that compromised personal data associated with *hundreds of millions* of credit and debit cards. Among New Yorkers alone, 22.8 million private records have been exposed, the result of data breaches from the past eight years at businesses and government agencies, announced Eric Schneiderman, New York's attorney general, in a July 2014 report.

"As we increasingly share our personal information with stores, restaurants, health care providers and other organizations, we should be able to enjoy the benefits of new technology without putting ourselves at risk," Schneiderman said. His recommendation?

"I will advocate for collaboration between industry and security experts to ensure that organizations across the state and country have access to the tools needed to secure our data, so we can best address this complex and growing problem."

Apple Pay is the culmination of one such effort, incorporating tokenization that removes a credit or debit card's PAN (primary account number) — and replaces it with a random string of characters, or a token, that is only revealed when it reaches a payment network. Another important aspect of Apple Pay is that it is not an encrypted value and therefore cannot be decrypted by thieves.

As a result, when Apple Pay is initiated during a transaction, the merchant never collects user-specific data. Only a payment network and the card user's bank retain information about the specific transaction. As for the token, it is worthless to a hacker, as it bears no association to a card user's PAN (and the token typically expires after the purchase, too).

While tokenization is not a new process, with Apple's track record as a technology trendsetter, it promises to accelerate and enhance its likelihood of industry acceptance. And with every emerging technology comes industry standards, which affect liability and compliance costs.

All of this makes tokenization highly relevant for you to consider as you assess the best way to protect your customers and your brand.

History of Tokenization

With Apple Pay, Apple has introduced a tokenization iteration that is stored on a smartphone. However, it is far from the first company to leverage tokenization technology. "This system is not new," explained Gray Taylor, executive director of Conexxus, writing for *MAG Quarterly*. "ExxonMobil's Speedpass has been using tokens for almost 20 years."

Over the past several years, vendors have come forward offering proprietary tokenization services. First Data launched its TransArmor solution in 2010, which offers end-to-end encryption as well as tokenization to protect cardholder data, a

More importantly, merchants that use third-party tokenization substantially reduce the risk of data theft — something PCI does not directly address.

comprehensive protection scheme that is resonating among retailers. "In just five years, TransArmor has tokenized 4 billion transactions for more than 700,000 merchants," said Paul Kleinschnitz, senior vice president of cybersecurity solutions for First Data.

Companies that implement a third-party tokenization program such as TransArmor can take advantage of a streamlined version of the Payment Industry Data Security Standard (PCI DSS) assessment, a concession that reflects the inherent strength of tokenization technology. Perhaps more importantly, merchants that use services like this substantially reduce the risk of data theft — something PCI does not directly address.

NOT JUST PAYMENTS

While Apple Pay has shined a light on tokenization for mobile payments, its application extends far beyond credit and debit cards. "Tokenization can be used for other types of data: protecting social security numbers, driver's license numbers and addresses, even medical records," said Steve Stevens, executive director of ASC X9, an organization that develops technical financial industry standards. "While at the moment the biggest users of tokens are the credit card companies, the technology is still in its infancy. In 10 years, you'll see a tremendous use of tokens. We're just getting started."

"Banks have known for years that fraudulently opened (by identity takeover) accounts can flourish in a tokenized payment system," said Gray Taylor, executive director of Conexxus. "This is a key reason why it is imperative our society expand tokenization standards to include all forms of personally identifiable information, of which card data is just one example, to prevent all forms of data theft."

DEADLINE APPROACHING

By October of this year, liability for counterfeit fraud shifts to retailers who have not adopted contact chip terminals if a dual-interface or chip card is presented for payment.

RECOMMENDATIONS

In March, the Merchant Advisory Group published (with support of NACS and Conexxus) tokenization recommendations that stress:

- Open standards development and interoperability
- The deployment of the most effective security solutions
- Fostering a competitive environment under which the technology is accessible, affordable, and able to evolve with marketplace demands
- Ensuring common sense business operations and data management

For more information, visit www.merchantadvisorygroup.org and www.conexxus.org.

Interchange 2.0?

Tokenization is a "game changer," according to Taylor, with the ability to reduce security risk in the future payments landscape. As such, "We should be spending our time on tokenization and encryption — together, they offer the most enhanced protections, far beyond what PCI and EMV offer. In fact, with [tokenization and encryption], EMV might not even be relevant." But it's not full speed ahead, Taylor said, as he cautions that adoption carries "significant risks."

"Tokenization introduced without oversight has the potential to become the new 'interchange,'" Taylor said — a vulnerability that has insiders already on edge.

Commensurate with the adoption of tokenization is the introduction of standards, which provide guidance for usage. Earlier this year, EMVCo, the organization that manages the Europay, MasterCard, Visa (EMV) chip card standard, introduced its own proprietary standards, which were adopted by Apple Pay.

"Apple Pay introduced the latest iteration of payment tokens by using format preserving EMVCo-compliant tokens stored on the secure element of the iPhone 6," Taylor said. "These tokens are currently generated and managed by the card brands, and ... the inability for the tokens to be introduced without an iPhone or reused at other merchants who did not initiate an Apple Pay transaction make them inherently safer."

However, there's a "dark side to the Apple Pay story," as Taylor pointed out. "Tokenization is good and should be embraced quickly, but the token format and provider role should be open and available to any trusted provider a merchant (or consumer) chooses to use." Not just EMVCo, which is controlled by the card brands — the same card brands that have dictated interchange fees (pre-Durbin), as well as PCI and EMV compliance standards, three long-standing industry issues.

"We can see the pain that PCI has cost us," said Phil Schwartz, manager I/S, credit card systems POS app support for Valero Payment Services Company. "Generally, the card brands have been beating up on the merchants to try to secure what was originally given to them as a faulty product. The mag stripe credit card is the source of the problem. But who was getting blamed for the lack of security? Merchants."

Where's Your Data?

Another downside to tokenization is a loss of customer data, a substantial concession. "If you own the token, you own the

data," Schwartz said. "Which means that if you set the standard for the token and create it, you gain the customer information."

With Apple Pay and EMVCo tokenization in its infancy, attention has not been given to data control — which is all the more reason to be concerned, said Mark Horwedel, CEO of the Merchant Advisory Group (MAG). "Once we at MAG understood tokenization and what Visa and MasterCard intended to do with it with EMVCo, we had concerns," he said. "People think losing access to data surrounding payments is as big an issue as interchange. Merchants need to consider this before they just jump in and accept them." All of which promises to heat up internal debate in larger companies.

"While marketing folks tend to embrace new developments, treasury folks are more cautious. They should remind marketing people that you've spent years building analytics around measuring customers. Prepare to throw that investment out the window and prepare to budget to buy that info back from the banks and the networks with tokenization," Horwedel said.

A Standards Approach

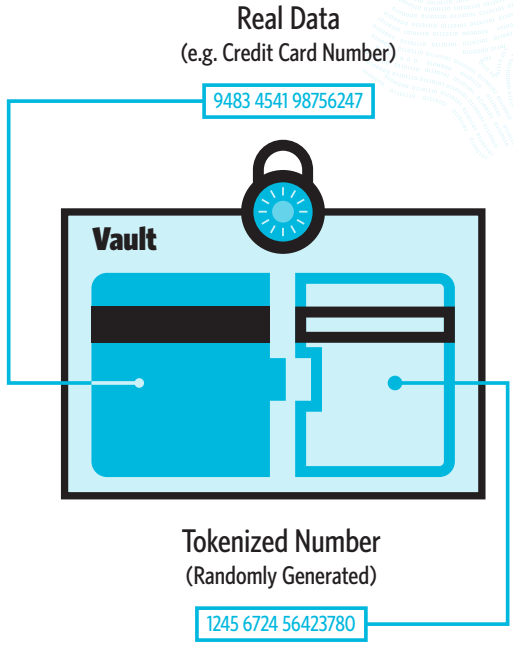
All of which points to the need for standardization, said Steve Stevens, executive director of ASC X9, an organization that develops technical financial industry standards. "Especially because of [the value of] applying tokenization to other data, the standards shouldn't belong to the card networks. They should be developed by an open organization where the applications are not just for payments but for all forms of sensitive data that should be tokenized."

NACS, working with Conexxus, has aligned with other retail organizations such as MAG and is advocating for open standards, not those dictated by the card brands, "to ensure that the potential societal value of tokenized payments (and other data) does not come with subjugation to new monopoly powers," Taylor said. Their collective goal? "To ensure that next generation payments operate in the light of competition and not as a replacement for interchange pricing power."

For now, there's EMVCo's Payment Tokenization Specifications, as well as competing models by The Clearing House, Payment Card Industry Security Standards Council, and the Accredited Standards Committee X9 (ASC X9). ASC X9 is a standards body accredited by the American National Standards Institute (ANSI), which has been developing financial standards for the financial services industry for more than 30 years.

ASC X9 is finalizing its tokenization standard (119.2), which it intends to release this summer, and is predicated on open standards. "In the open standards world, you have lots of people who can look at things and ask whether you thought about a certain scenario," Stevens said. "When you're done, hopefully you've got an economical solution where you've thought about what the hackers will think about and you've plugged the holes ahead of time. If you have a single company looking at things, you can miss things."

Tokenization Process



Secure token vault with link between real and token values, hosted in-house in a company's data center or by a third party vendor or cloud provider.

MAG released a set of its own tokenization recommendations in March, which also argued for open standards. "Tokenization technology has the potential to provide the greatest level of protection against fraud, enhance competition and provide the highest level of return on investment for commercial stakeholders," Horwedel said. "Given the existing unhealthy level of market concentration in the payments industry, it is imperative that tokenization standards be developed in an open standards environment in order to ensure a competitive landscape under which the technology and all payments stakeholders can evolve and deploy the most effective data security measures for the benefit of U.S. businesses and consumers."

Looking Ahead

Of course, as with any technology that promises a more secure shopping experience, the hackers have indeed found a loophole. And so it is with Apple Pay.

A worker inside a mobile kiosk sponsored by Visa and Wells Fargo demonstrates the Apple Pay mobile payment system.

According to news reports, criminals have been increasingly adding stolen payment card data to their iPhones (no word if the phones were stolen, too) to make in-store purchases. "Instead of stealing payment data from Apple Pay users, these guys get the sensitive information from another source and then use Apple Pay to turn it into goods," reported *CIO Magazine*. "I don't think [anyone] saw this one coming."

It's not going to be the merchants or the card brands that pick Apple Pay or something else. Consumers will pick the next payment system.

While this doesn't speak to the vulnerability of tokenization, it has brought a negative association to Apple Pay, which could slow down consumer adoption. And as we've seen with previous mobile payment platforms, their success depends on whether shoppers will ditch their credit and debit cards for the bright and shiny mobile wallet.

"While Apple Pay is pretty nifty, as to whether it becomes a viable concern for merchants right now, the interest is very low," Schwartz said. "There aren't that many people using it every day, and people aren't saying they'll avoid your store if you don't take it. Ultimately, it's not going to be the merchants or the card brands that pick Apple Pay or something else. Consumers will pick the next payment system."

Despite that cautious approach, Schwartz advocates for staying on top of the tokenization issue and to support open standards — whether Apple Pay succeeds or not. "It's the only way to get ahead of the card brands. We need to get involved and make sure we have representation at the table," he said.

No matter whether Apple Pay catches on and who sets tokenization standards, the bottom-line focus should be on data security, Kleinschnitz said, and for that, tokenization is a valuable process that retailers should embrace. "The criminal threats are increasing up to 300% each year," Kleinschnitz said. "As a retailer, you want better protection than others because criminals look for the least resistance.

"You never want to be the last guy chased by the bear." NACS

Jerry Soverinsky is a Chicago-based freelance writer. He's also a NACS Magazine *contributing writer.*

Rethink the Refill

New Research on Dispensed Beverages

A recently completed research study conducted by NACS and Whirley-DrinkWorks! with existing c-store customers has generated refreshing new insights on what drives consumer frequency and loyalty for dispensed beverages, and the role refill programs play.

NACS Shopper Panel

Whirley DrinkWorks!™

VISITS

C-stores have most repeat visits/week to purchase dispensed beverages.

LOYALTY

#Love MyMug

Over 30% of refill mug users participate in a beverage loyalty program

BASKET

Beverage loyalty program participants buy more items and spend more $.

Put Your Refill Program to Work!

Go to WhirleyDrinkWorks.com/Research for a FREE research summary brochure.

Whirley DrinkWorks!™