PAYMENT INDUSTRY'S TAKE ON TOKENIZATION

A PYMNTS.COM REPORT

TABLE OF CONTENTS

CHAPTER 1...

SEVEN INDUSTRY PLAYERS OFFER THEIR TAKE ON TOKENS

SEVEN INDUSTRY PLAYERS OFFER THEIR TAKE ON TOKENS...

The use of tokens – the concept of a surrogate being used to replace something of value – is nothing new in payments and financial services. But the consumer-driven demand for smart devices, coupled with rapidly changing technologies, has the industry buzzing about what's next in tokenization – especially when network tokenization, at least for now, seems a bit at cross purposes with tokenization on the acquiring side.

Hardly has there been a topic that has garnered as much attention across the payments ecosystem as tokenization has recently. It's not a new concept, since tokens have been used to encrypt cardholder information post-authorization for many years. But it's one that has cast a new light on the role of the various stakeholders across the payments ecosystem with the introduction of network tokenization that replace payments account numbers when payments transactions are initiated.

These tokens are presented to merchants for payment, and enabled for payment by a new player – a Token Services Provider – that authorizes the payment. Payments tokens, as some refer to them, are stored in vaults maintained by the TSP – which could be an independent third party or integrated with the card networks.

Seven senior executives from across the payments and commerce landscape, each representing a difference facet of the industry, came together on the evolution of tokens and tokenization. The focus was how this developing technology can be used to facilitate a demand for payments that are both secure and convenient.

TOKENS BEFORE TOKENS WERE COOL

Starting with the perspective that the payments industry was all about tokens before tokens became cool, thanks to the introduction of Apple Pay.

"Apple did not invent tokenization, it has been there for a long time. What is now happening is, that its use is now standardized for all payment cards across the world. The stumbling block earlier was making sure a card that is tokenized by one player in the U.S. works in the U.K., and that is what network tokenization brought to us," said Hitesh Anand, VP of Commerce Enablement and Mobile at Verifone.

TOKENS — EVERYWHERE YOU WANT THEM TO BE?

True enough, everyone agreed. But we have the *"battle of the tokens"* – tokens on the acquiring side that don't have anything to do with tokens on the payments and issuing side. Tokens, some believe, need to be ubiquitous – enabling payments to be made anywhere and everywhere – to deliver the promise of payments safety and security. Yet with ubiquity comes many questions and challenges.

"Only when we can deliver these tokens ubiquitously, can we get to a point where we can start changing consumers' behavior from what they normally use for payments which is swiping or dipping a card, to utilizing their mobile devices to use tokenization for payments. Without that behavior change, it's going to be very hard for tokenization to take off," added Will Graylin, CEO of LoopPay and Co-GM of Samsung Pay.

WHO GIVES A TOKEN?

Customers accepting and using tokenization may be a large hurdle, but opinions differed around how significant consumer behavior really is when it comes to growing the use of tokens. As many of the panelists pointed out, consumers are less likely to understand the concept of tokenization itself. Instead, they remain focused on being able to make payments in a way that is convenient and innovative, but also secure.

A position that Alex Pezold, Co-Founder and CEO at TokenEx — a technology platform that provides tokenization — was passionate about. Sure, security is a key value proposition, but shouldn't that be the driving force, and not how the industry proposes to create that?

"One of the questions that I have on trying to change consumer behavior with tokenization would be is that the tail wagging the dog? **Consumers really don't care about tokenization, they care about security, they care about the really cool fingerprint that you put on your Apple or Samsung device.** Where this really is applicable is trying to secure and trying to help merchants and service providers with compliance, risk and fraud reduction," Pezold said.

Verifone's Anand agreed, but took things a step further. "When we use the word tokenization we are at times guilty ourselves of using it only in the context where the consumer is the focus. There are other contexts where the consumer is not making that choice or decision and we need to make sure that tokenization importance or benefits in those areas are seen as just as valuable as on the issuer side," Anand added.

THE TOKEN INSIDE

As smartphones continue to flood the market, the panelists debated whether tokenization can keep pace with the growth of mobile. Changing mobile technologies are allowing consumers to do more on their devices than ever before, which may provide an opportunity for tokens to be used in innovative ways.

“The ubiquity of the mobile device allows the customer to bring their own container, as long as the container provider makes sure it’s secure so the customer can pick their own end points and link them all to a funding account they have,” said Doc Vaidhyanathan, VP of Product Management and Digital Payments at CA Technologies.

Vaidhyanathan pointed to the importance of providers identifying whether a particular end point can be provisioned or not, as well as assessing the risks associated with trying to alter a token.

“This allows for a whole lot of customization of that token, as far as when it can be used, where it can be used, for what purpose can it be used. It also provides opportunities for controlling the spend, controlling the fraud, as well as creating new exciting uses for the token,” he added.

CAN’T WE ALL JUST GET ALONG?

How do payments and security tokens live together? How does the introduction of payments tokens and mobile payments change what networks, acquirers, issuers and payments services providers do? How will mobile commerce players adapt today?

Despite the variety of opinions on the topic, there was one point of agreement: Tokenization not only provides significant growth in digital payments but also does so in a way that is both consistent and convenient.

“There is a demand from consumers to be able to pay where they want, how they want, when they want, and with whatever card they happen to have. Tokenizing for us is an enablement of all these different payments experiences that are possible and doing it an incredibly secure way, which helps us to create experiences that couldn’t actually be enabled without the arrival of tokenization,” explained Matt Barr, Group Head of MasterCard’s Emerging Payments in the U.S.

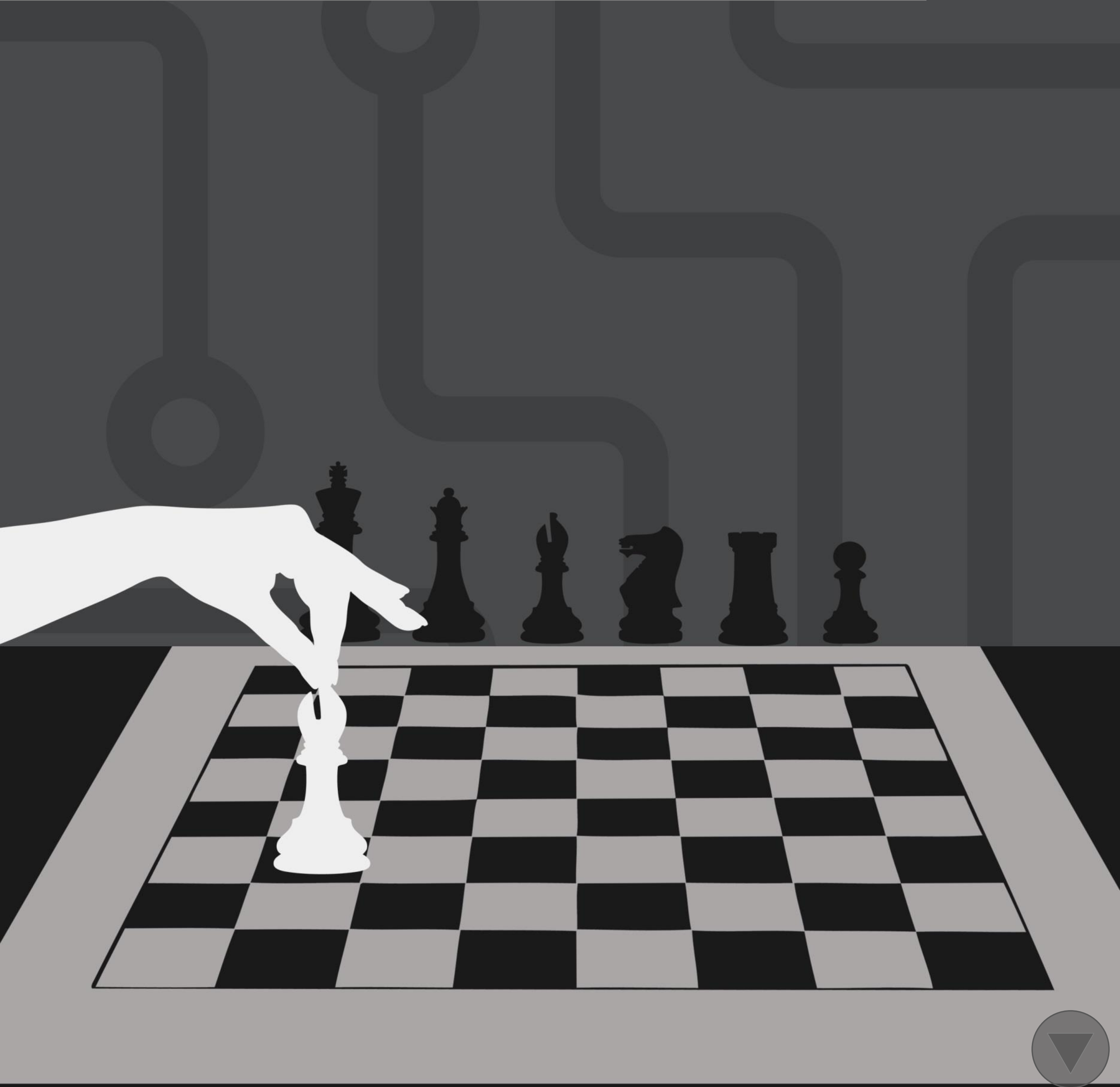
“We are seeing leveraging of newer tokens for secure in-app purchases and have heard talks to the future of enabling that same level of security for browser-based eCommerce, which we know we have to secure as EMV arrives in the U.S., so all of these channels must become secure and in a way that has backwards compatibility and is globally interoperable,” Barr said.

According to Barr, there has been encouraging momentum across payment methods, from both a consumer and merchant perspective, and the key enabler in that acceleration has been tokenization.

CHAPTER 2...

HERE A TOKEN, THERE A TOKEN

ONE-ON-ONE WITH ALEX PEZOLD, CO-FOUNDER AND CEO OF TOKENEX



HERE A TOKEN, THERE A TOKEN…

Tokenization may not be new, but it is a hot topic in payments, thanks to the introduction of the network tokenization schemes. All of this is pulling merchants in a variety of directions to understand what to support and why and when.

Alex Pezold, Co-founder and CEO of TokenEx, doesn't think merchants should be locked into any one solution, as flexibility is the key to success in a world of tokenization. He shared his thoughts on the matter in a discussion with MPD CEO Karen Webster.

KW: Tokenization has become very much a buzzword, with everybody throwing it around. There are actually two tokenization camps: the security tokens that protect the data at rest once it's traveled through the point of sale environment on the acquiring side, and the payment tokens on the issuing side that the networks have created to enable payment schemes such as Apple Pay, Android Pay and the like.

On which side of the token universe is TokenEx?

AP: TokenEx is actually on both sides of the fence. We have customers, for example, that are digital wallets, that are using TokenEx and our platform very much like Apple Pay uses Visa, and how MasterCard is applying tokenization to the digital eCommerce marketplace.

But we also have lots of conversations with big players in the retail and eCommerce arena who are fed up with being tied to the existing payments players. They're fine with having multiple providers for separate services – like fraud prevention, and tokenization, and so on – they just don't want to be bound to contracts and pricing with any one of them. They want the flexibility to maneuver between different providers.

TokenEx addresses that need, providing tokenization for customers who are tokenizing payment card data, personal identifiable data, and any number of different data sets that present risk for data at rest, as well as architectures for mobile payment platforms that are available.

KW: Who are your customers? Who actually buys the token platform services that you offer?

AP: Think of TokenEx as a layer of abstraction between merchants and service providers and the payment service providers. Small- and medium-sized businesses tend to buy us for the compliance component; they want to reduce or even eliminate compliance. Larger organizations, such as Fortune 500s, will buy us because they want to get rid of risk. Our customer base ranges from startup eCommerce platforms all the way to Fortune 10 companies.

Our target market, and where we see a tremendous amount of growth right now, is eTailers that have multiple payment acceptance channels. For them, we act not just as a tokenization provider but more of data security platform and a tokenization integrator, regardless of the size of the particular company.

KW: Something you said that I found interesting was that your customers want the flexibility of not having to be tied to a single provider of payment solutions. The flipside of that coin, though, is that having one provider really does simplify things – especially for merchants that otherwise lack the resources and know-how to go to different places for different services.

How do you simplify the conversation with – and the solution for – a merchant that has a lot of other things to worry about?

AP: That's a great question. I mentioned the term "integrator," which describes how we view ourselves with respect to tokenization encryption and key management technologies, as opposed to simply a tokenization service provider.

We've moved ourselves out of the latter category because it assumes that what every commoditized payment service provider is putting forth today is the tokenization generation engine.

Simplifying the conversation is very easy to do. We ask the merchants, "What are you trying to achieve?" They want to be as many places as they possibly can be to acquire as many transactions, or purchases – whatever the specific metric may be – as possible. The goal for us becomes to get as close as possible to the payment information in that channel, while the merchant maintains whatever service providers it chooses.

If a merchant wants to have an all-in-one provider for fraud solutions, it can do that. But we recommend that the merchant still give itself some flexibility to maneuver – at the very least, keeping its data away from the provider.

We're integrated with over 30 payment gateways, 4 of the major 7 payment processers, as well as with fraud prevention solutions. We aren't just providing services; we're providing a complete solution for customers. And that often includes solutions that help direct them to different providers that best fit their needs for different services.

KW: So you give them the ability to unbundle the tokenization service from other services that their acquirer may offer, and they can take the risk-management piece of that payment capability wherever they like. Is that the pitch?

AP: "Unlimited flexibility" is the pitch.

And when we offer flexibility among any service providers, we include ourselves in that. We don't require contracts; we will give our customers back their data with 24 to 48 hours; should a customer decide to bring a tokenization capability or an encryption capability in-house, we'll gladly help them with that transition away from us.

That's just the way we choose to do business. We want things to be flexible and easy for our customers – no hang ups; no situations where we're holding data hostage. Business shouldn't be done that way; it should be very transparent and easy, as to serve the best interests of our customers' livelihood.

KW: The excitement is generated because you give them flexibility, and you minimize PCI scope… But don't a lot of other people do that, too?

AP: No, not necessarily. And I would say the excitement for these companies actually comes from the creativity and the freshness of having a true integrator working with them, as opposed to just a platform provider.

We tell our clients, "we're going to connect and we're going to push your PCI compliance boundary to the furthest edge." Most payment service providers can't say that.

If a company is looking to reduce compliance scope and uses a standard service provider, that provider is going to give you a solution – maybe. They'll perhaps solve an eCommerce problem, but they won't solve a call center problem, or a mobile problem; they won't solve batch files or a virtual terminal. Payment card data still has to flow through a merchant's environment before it can be sent off to the processor, so their entire environment is still in scope.

With TokenEx, we're actually going beyond that. We're pushing way out to the boundary and all those different acceptance channels. And that's what gets companies excited.

KW: The way that tokenization and related activity works within the payments ecosystem seems very fragmented today, with lots of different people doing lots of different things. Do you think that at some point a standard will be established that brings it all together?

AP: I don't think so; and I would actually submit that that's an undesirable outcome.

Were tokenization to be standardized, with everyone using it in the same way, that would actually amount to just a recreation of credit cards.

KW: Standardization, though, is what makes credit cards work globally.

AP: Exactly – and the problem with credit cards right now is fraud and security. If somebody steals a credit card, he or she knows that it can be used just about anywhere.

If a token is created that looks like a credit card across every single service provider, then it can, in essence, be used as a credit card. A cross-domain tokenization issue is created.

I think that EMVCo, The Clearing House and PCI are all doing a great job of defining what is acceptable in terms of how tokens should be created for various implementations. The industry was already several years into providing tokenization before any of those three entities actually pushed out any type of guidance. You don't want to create that cross-domain issue with tokens, so it's good that it's fractionalized because that prevents one token built for one service provider being used with another service provider.

KW: But aren't the networks solving for that – by separating the payment tokens from the transaction tokens? And then applying a cryptogram to?

They're not issuing the same token for everything, but they're creating an underlying standard that everyone can in turn leverage in order to create consistency around the world.

AP: Standardization as it pertains to communication and usage is totally fine. It's a different case for standardizing token generation because every environment is unique – which segment of the card number is retained, whether alphanumerics are applied, and on and on. For a merchant or service provider that's already tokenized its entire environment to suddenly be told, "that's not going to work anymore," that won't fly and they'll just continue to use independent providers.

As far as the way that tokens are utilized and passed around in different ecosystems, I think it's good to have some kind of guidelines to go by. Not so much with the generation of the actual token.

KW: We're certainly in early days. But there's a whole new path being laid out by the networks with their digital enablement services that tokenize on the issuing side, standardizing it, and removing the provisioning burden from issuers in order to get some traction with mobile schemes. It's obviously a hot topic, as evident in what you just described.

AP: Love it or hate it, Visa and MasterCard aren't going anywhere. They're going to continue developing new ways to retain business. As each tries to design a framework for the digital ecosystem in its own way, neither is exactly playing nice – they're not meeting in the middle. If there is going to be a standard for communication and usage, those guys will need to get on the same page.

KW: At the end of the day, the goal is ultimately to keep data secure and create confidence in how payments transactions are done. Turning back to the merchant side, I feel for the merchants who are trying to sort it all out. They have so much coming at them today.

AP: I feel sorry for merchants today. The one voice they have repeatedly telling them that they need to be PCI compliant is from their upstream – their payment service provider, whoever that may be. But that same upstream isn't providing any guidance for the process.

If I had a penny for every call I've had with one of our customers about their payment service provider talking about PCI compliance and how to validate for it, I wouldn't need to have a tokenization company – I'd be rich!

The reality of the situation is, customers are being told that they need to be PCI compliant and simply directed to a website or given a form. Nine times out of 10, that form is the wrong form – so the customer is immediately out of compliance and at risk. In my experience, payment service providers and upstreams are not giving sufficient guidance in terms of the steps needed in order to achieve compliance.

We have those conversations with customers; we educate them about the details specific to their situations and it alleviates frustration about the process. Merchants ultimately want to have these conversations; it's just that payment service providers so often treat them as if they're an annoyance.

KW: Let's say you're sitting across the table from a merchant, and the merchant says, "I am bewildered. I have EMV coming at me and I've got to figure out what to do there.

I'm hearing everyone talking about their respective tokenization services; I have people wanting me to rethink my POS environment and buy new hardware.

"What's my first step? If I do one thing right now to give me the best possible protection of cardholder data, what should it be?"

AP: That's actually a really good question. The easiest thing that comes to mind would be for the merchant to get rid of that big glut of credit card data it's storing in its environment for recurring payments, analytics, customer convenience or the like. A data breach would cost the merchant about $90 per record – so multiply the whole thing by 90. That data needs to go.

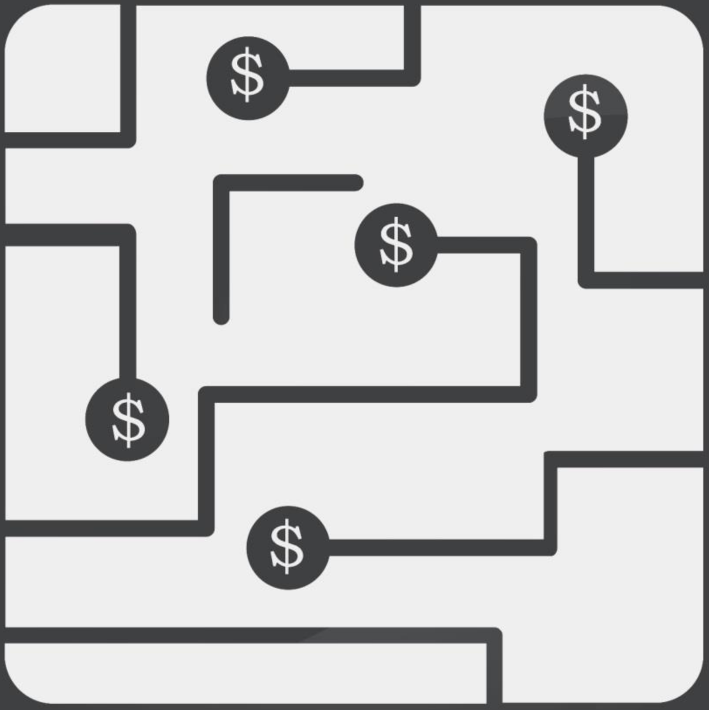
Beyond that, I would recommend sitting down with the merchant to map out its data flows and the technologies associated with them. Then we'd talk about the technologies being introduced today that are going to match up with EMV, or PCI, or any of the different things the merchant is trying to do – such as mobile.

From that point, we can discuss a phased strategy for rolling out technologies that, No. 1, are going to make sense for the merchant and that's comfortable using, and, No. 2, aren't going to break the merchant's bank.

KW: And there's a "No. 3" that takes us back to where we started: a technology that is not going to bind the merchant to a point-in-time technology that might be good for today but might not work as the business evolves. The fact is that businesses don't remain static if they're successful. They grow, they evolve, their needs and goals change. Having the ability to adapt is a pretty important requirement.

AP: I couldn't have said it better myself. As a business owner, you don't want to be locked into any one particular thing if you don't have to be. Doing business with who you want to do business with is actually a luxury these days; it's no longer a given.

In our experience, being a service provider that actually gives you options is certainly well-received.



CHAPTER 3…

TOKENIZATION GOES PRIVATE LABEL

INSIGHT FROM MASTERCARD, SYNCHRONY FINANCIAL AND BJ'S

TOKENIZATION GOES PRIVATE LABEL. . .

MasterCard is the first network to add tokenization support for private label (store-branded) credit cards was nothing if not big. Among the first retailers to participate will be BJ's Wholesale Club, JCPenney and Kohl's. The banks on board will include Synchrony Financial, Citi Retail Services and Comenity, a bank subsidiary of Alliance Data's card services business.

That's already a lot going on, so MPD CEO Karen Webster couldn't talk about the details of this breakthrough with just one person. Instead, she spoke with three different individuals, all of whom are very close to the action — albeit from different angles. **Ed McLaughlin, Chief Emerging Payments Officer at MasterCard**, talked about the plan; **Carol Juel, Chief Information Officer at Synchrony Financial**, broke down the nuts and bolts; and **Bill Werner, Senior Vice President of Finance at BJ's Wholesale Club**, provided a view from the merchant floor.

THE MASTER MIND - MASTERCARD

"A huge win for MasterCard."

Those are Karen Webster's words — spoken to Ed McLaughlin, Chief Emerging Payments Officer at MasterCard – about the network becoming the first to add tokenization support for private label credit cards for use in digital wallets.

The big breakthrough? McLaughlin agrees with Webster that it was MasterCard creating the NFC spec that private label cards can now use to enable mobile payments at the physical point of sale.

"In working with a lot of merchants," he tells her, "[we learned that] they had an investment in their private label portfolio. Some of their most dedicated customers, obviously, like to use their private label cards. For them to introduce payments innovation using the mobile device, they also wanted to make sure that they could also extend and offer that innovation to their most dedicated customers."

With the new mechanism in place, retailers like Kohl's, JCPenney, BJ's Wholesale Club and others now can enable those private label cards in that way. McLaughlin says that these companies are opening up to accept contactless payments "with great enthusiasm."

Additionally, customers who still want to use open-loop MasterCard payments products in the store can do so with ease. To facilitate the transaction — which operates by having MasterCard pass the tokenized account number to the issuing bank, which then processes it along its rails as usual — McLaughlin shares that his company has been working closely with the "elite set of issuer processors" that specialize in private label.

“From the start, our MDES [MasterCard Digital Enablement Service] system was always fully Durbin compliant,” which is to say that the support capabilities for routing and alternate networks were already in position. “It wasn’t that far to take what we had done to support alternate routing on debit cards [and] say, ‘Here’s how we can route the private label transactions while still providing all the security, while still doing the interface into the various wallets that will hold it’ — whether it’s an Apple, or a Samsung, or an Android Pay transaction — or any of the others.”

In putting the system together, MasterCard made sure not to disrupt the rewards and redemption elements that merchants have in place for their private label customers. Using the example of a debit card, McLaughlin explains that, after the token used for a transaction passes back into the system, MasterCard has already translated it to the underlying identifier — ergo, the specific and proprietary value is maintained.

There’s no issue with degradation of the data, either. Says McLaughlin, “We’re providing the service to enable the mobile environments, but it is backward compatible with the systems they have in place.”

Another bonus for MasterCard, in McLaughlin’s opinion, is that the private label tokenization service is providing a better understanding throughout the industry of MDES’ capability for multiple applications and, as a result, a wider appreciation for the value of its tokenization process.

“One important thing we’ve always honored is [that] merchants want to serve all of their customers,” McLaughlin remarks. “Whatever handset that customer happens to have chosen — for all sorts of reasons, whatever best fits their life — we can enable it.”

By enabling tokenization for private label cardholders, MasterCard may have removed the final obstacle for merchants to widely adopt mobile payments. While private label customers are a small percentage of the overall consumer base, they are nonetheless a particularly valuable subset — one that merchants are keenly interested in keeping happy.

McLaughlin actually sees opportunities for the merchants’ profitability from that “dedicated cohort of consumers” to increase, as they can now move some of them into an open-loop co-branded program.

A lot of other issuer-processors, says McLaughlin, “are very attuned to what their merchants want to do. So we think this will be really compelling for lots of merchants” as those organizations come calling, interested in getting in on the private label tokenization action.

To do that, they might want to get a fuller understanding of how the system works “under the hood,” so to speak — just as Webster herself sought. For that inside look, we turn to Carol Juel, Chief Information Officer at Synchrony Financial.

"Obviously," Juel tells Webster, "private label transactions do operate a bit differently than your normal MasterCard, Visa, Discover and Amex transactions." Juel characterizes that "difference" as the strong value proposition along with data, that is a critical incentive for consumers to use and a critical capability for rewards to be fulfilled at the point of sale.

"It's very important for [Synchrony] to ensure that we maintain the value proposition of our card as we work with the many new mobile payments innovators emerging throughout the various ecosystems that are emerging."

Synchrony has been working closely with MasterCard to enable its cards to work within Apple Pay, leveraging its tokenization services. Doing so allows Synchrony to tokenize its private label cards through the MasterCard process, while at the same time getting what it requires from a private label transaction to fulfill value proposition-related commitments to its customers, merchants and retailers.

The process, Juel explains, required Synchrony do to a great deal of work to code to the MasterCard spec, ultimately resulting in tokenization into BIN ranges — a necessary aspect for Synchrony to be able to leverage for its private label cards across its private label network.

As for solving for merchants' concerns about tokenization schemes potentially limiting their access to customer data — an essential aspect in servicing private label cardholders — Juel points to the level of integration that Synchrony has with the retail process at the point of sale.

"Our business is B2B2C," she states, "so the way we bring value to our retail partners is by bringing programs that help them drive their sales. And in doing that, they've created an interface with us that has data that helps us to fulfill those value propositions — the data that's provided at the point of sale transaction, as well as data that's provided from a settlement transaction — to ensure that we [can] meet that. So working through the process of creating that transaction as it flows to us over our rails is part of the integration that occurs with the retail partner."

It's a more complicated process than there is with a traditional bankcard because of the number of players involved. There's Apple as the hardware piece — as well as the operating system — there's the retailer, there's MasterCard and then there's Synchrony.

"It's really a four-party process that [is required] to understand the difference in the transaction," says Juel. "Each person has a really strong view on the transaction and what pieces are important to them in ensuring … that it flows as it needs to." In the transactional relationship between MasterCard, Synchrony and the retailer, the actual tokenization process tends to be divvied up among the three.

"There are services that MasterCard provides [as part of MDES] for decrypting and encrypting tokens," Juel tells Webster, "but we [also] use tokenization in places throughout our processing network … [and] most of our retail partners are working at tokenization at the point of sale. So in some cases you actually have tokenization of a token — this is where it gets a bit technical."

A bit? "It's the kind of stuff that can make your head spin," says Webster.

Apple Pay did not initially go to market with the capability for loyalty offers to be redeemed at the point of sale. The service has since been enhanced to accommodate that need, but Webster is curious to know if those enhancements are sufficient to enable private label card rewards.

"I can't really answer for Apple," is Juel's answer — although only in part.

She goes on to explain that there is a distinction between how loyalty rewards and promotions operate within the private label space and how they operate outside of it. For retailers that are integrated with Synchrony — Juel cites the example of JCPenney, a partner with the bank — much of the logic related to promotion processing is already built into their transaction systems. All they have to do is be able to code for the Apple Pay transaction in order to redeem loyalty offers via that system.

While JCPenney, Kohl's and other retailers are no doubt excited to be able to offer tokenization capability on private label cards, the operation didn't exactly come together overnight. Juel estimates that it took six or seven months to achieve full implementation.

What actually helped keep it from taking even longer, she says, is Synchrony's longstanding relationships with both MasterCard and JCPenney. Those three entities together were actually able to help Apple Pay gain the necessary understanding of the private label card business.

"All the parties were aligned in solving the problem," Juel remarks.

The plan is for Synchrony-issued private label cards within Apple Pay to be available to consumers of JCPenney and other retailers in the fall. Juel has little doubt that a lot of merchants will be watching closely, anxious to turn on the capability for themselves.

"We're very excited about it," she says but is quick to tell Webster that Synchrony is mobile wallet agnostic. "We support a large number of merchants and retailers and wallets across the U.S."

The company is not in the business of predicting a winner among those, explains Juel, because "ultimately we feel that consumers will decide." You know who might know something about consumers? The final stop for Webster on this trilogy of interviews: Bill Werner, Senior Vice President of Finance at BJ's Wholesale Club.

What makes things a little easier for BJ's to hook up with MasterCard's mobile wallet tokenization scheme is that its store card is already a co-branded one with MasterCard. A little easier — notes Werner — not a lot. Because, MasterCard affiliation aside, through Comenity, a bank subsidiary of Alliance Data's card services business, BJ's card is more or less treated as a private label card in-club.

"We just launched our product in October, so some of the bells and whistles are kind of still to come," Werner remarks. "But one of the things that we … want to have the ability to do is offer our members the more 'private label' type of promotional stuff on the card — like double points and zero percent financing on certain purchases. In order to enable [those things], you need a more direct connection with the bank than you would get … authorizing and settling it over the MasterCard rails, which is why we opted for a co-branded and not a private label product."

Building those data-dependent enhanced features into a preexisting co-branded card, he says, proved something of a challenge. The company had to sort out how to navigate alternating card numbers generated by tokens (the token of a token issue mentioned by Juel earlier), and enhanced security features embedded in the transaction. Those steps enable that very security while remaining capable of identifying the transaction and getting Comenity the information it needs to ensure BJ's has the same experience with Apple Pay that it does when somebody swipes (or taps) a physical card.

The key, Werner tells Webster, is "making sure that the bank is able to affect the process on the back end so that we can first get the token information to MasterCard to decrypt the transaction and get the payment credentials, and also get that information over to Comenity with the enhanced settlement data to complete the transaction." He acknowledges that he's probably not as worried as other merchants are about losing customer data or access to it, by virtue of the fact that BJ's is a membership club, so it already has all of that information on hand.

"The major problem we needed to solve for was just making sure that we could identify the transactions through the entire process to say, 'Hey, double-bonus this transaction … give zero percent financing on this transaction," to make sure we maintain the flexibility. I would say that there was a great partnership between Comenity, MasterCard and Apple to work through a solution for us because they recognized that this was an important problem for BJ's to solve."

As a merchant, BJ's was already NFC-enabled before MasterCard's private label tokenization scheme came to its doorstep — in fact, the chain was one of the first launch merchants for Apple Pay. It got on board with MasterCard's plan because, as Werner explains, "we really wanted to make sure that … members who have the My BJ's Perks MasterCard, [who] are some of our most loyal members … had the same experience in-club as other members did."

That goal may speak to the reason why BJ's is less concerned with tracking the percentage of Apple Pay transactions within the scope of NFC (which, Werner notes, is "pretty slim") as it is with making the experience as convenient as possible for its customers.

Perhaps a little bit different from other membership clubs, Werner observes, "We try to make sure … that members can use any type of payment they want, any card they want."

There's a potential opportunity in that flexibility, Webster proffers, insofar as BJ's could attempt to stimulate more usage on the part of its members simply by having them put their co-branded cards in their Apple Pay wallets.

"It's no secret that what you want to get with the co-branded card is robust internal sales and more trips," acknowledges Werner. "But you also want to … make sure it's top-of-mind to people when they're shopping outside the club. We've developed what we think is a pretty good program to give people some good benefits, not only on what they spend inside of BJ's but also when they use that card in other stores, too."

With the industry in a frenzy over mobile payments, BJ's counts itself among the merchants that are getting solicitations from any number of providers looking to get a piece of Apple's pie, so to speak. Looking to the future, Werner says that the company is "prepared to support anything that is cost-neutral to us and gives our members … flexibility — and obviously maintains my flexibility as a merchant."

"I need to be giving my members the best experience I can every day," he adds, "so we'll gladly work with those partners."

He's quick to add, though, that because of his company's long partnership with its bank, "there's always good dialogue in terms of what we want to do."

CHAPTER 4...

EXCUTIVE CONCLUSIONS

TOKENEX, VERIFONE, DIGITAL RIVER, CA TECHNOLOGIES AND SAMSUNG PAY

EXECUTIVE CONCLUSIONS

To gain deeper insight into tokenization PYMNTS asked the question:

Q: From your perspective what issues surrounding tokenization still remain unaddressed?

HERE'S WHAT THEY HAD TO SAY...

TOKENEX

ALEX PEZOLD, CO-FOUNDER AND CEO

The issues I see surrounding tokenization that are still unaddressed have everything to do with education and empowerment to use this great technology for compliance reduction and risk reduction. While we're halfway through the year in 2015, if the only association people are making with tokenization is Apple Pay, then we have a long road ahead of us. If the card brands are using ubiquitous tokenization as a means to drive digital wallet adoption, then we have an even longer road ahead of us, because they apparently don't get it either.

For example, simply using a tokenization engine like what payment service providers and the card brands provide is not going to reduce PCI scope or risk challenges that merchants and service providers are facing today. Looking at the payments industry, the term "omnichannel" is present for a reason – merchants and service providers alike handle payment card data in any number of different channels. Only addressing one of these channels is not going to solve the problem of getting risky data out of a merchant's environment.

The payments industry needs further education around tokenization and understanding that it's not just a solution for payment service providers and the card brands. Tokenization is a solution for any organization handling any sensitive data set, like payment card data, personally identifiable data, or financial account data, who also uses any number of avenues to interact with said data.

Educating merchants and service providers alike in the areas of achieving/maintaining compliance and risk avoidance, and empowering them to use tokenization as a competitive advantage of sorts should be our continued goal and receive the attention it deserves.

VERIFONE

HITESH ANAND, VP OF COMMERCE ENABLEMENT & MOBILE

Tokenization, while important, is not a security catchall and should be used as part of a multi- layered approach to security that also incorporates end-to-end encryption and secure commerce architecture. Of course, large retailers likely have the resources and support in place to deploy and manage these types of systems. However, smaller merchants on the other hand may not have the necessary bandwidth or technical knowledge to do so on their own. That's why it's imperative for smaller merchants to partner with processors and acquirers offering managed payment services — also known as Payment as a Service — that incorporate all of the recommended components of effective multi-layered protection, which of course includes tokenization. Not only does this type of service greatly enhance payment security, it also shifts the burdens and complexity of payment system management away from the merchant, allowing them to focus more on their core business

DIGITAL RIVER

SREEMATI LALGUDI SESHASAYEE, DIRECTOR OF MERCHANT CONNECT

The issues I see surrounding tokenization that are still unaddressed have everything to do with education and empowerment to use this great technology for compliance reduction and risk reduction. While we're halfway through the year in 2015, if the only association people are making with tokenization is Apple Pay, then we have a long road ahead of us. If the card brands are using ubiquitous tokenization as a means to drive digital wallet adoption, then we have an even longer road ahead of us, because they apparently don't get it either.

For example, simply using a tokenization engine like what payment service providers and the card brands provide is not going to reduce PCI scope or risk challenges that merchants and service providers are facing today. Looking at the payments industry, the term "omnichannel" is present for a reason – merchants and service providers alike handle payment card data in any number of different channels. Only addressing one of these channels is not going to solve the problem of getting risky data out of a merchant's environment.

The payments industry needs further education around tokenization and understanding that it's not just a solution for payment service providers and the card brands. Tokenization is a solution for any organization handling any sensitive data set, like payment card data, personally identifiable data, or financial account data, who also uses any number of avenues to interact with said data.

Educating merchants and service providers alike in the areas of achieving/maintaining compliance and risk avoidance, and empowering them to use tokenization as a competitive advantage of sorts should be our continued goal and receive the attention it deserves.

CA TECHNOLOGIES

DOC VAIDHYANATHAN, VP OF PRODUCT MANAGEMENT

The issue that still remains unaddressed is the new tokenization, introduced with solutions like Apple Pay is the Payment Token (unlike the Acquirer Token used for PCI compliance and Issuer Token used to anonymize transactions). For now the Payment Tokens are generated by the networks only. The rules of engagement have not yet allowed third party token generators to be effective in this space.

Also, for now, Payment Tokens are being generated mainly to be put on Mobile Wallets. This has to be expanded to allow Payment Tokens that can be held and used in any channel. The cardholder currently has no say in what the properties of the token are – the networks have decided that the tokens put on iPhones are only usable for Apple Pay – but there is no fine grain control that the cardholder can exercise. The future has to include the cardholder as an influencer of what the token represents.

SAMSUNG PAY

WILL GRAYLIN, GM

The unaddressed issue to tokenization at this moment is the need for wide acceptance by merchants in the physical and the online environments, across merchants without heavy IT changes to their POS systems and to their remote checkout systems. This problem can be solved in the physical world with innovations like MST that Samsung Pay will be launching to enable existing POS to accept tokenized mobile payments without change.

For online tokenization, TSPs can also innovate by generating a timestamped 3- or 4-digits dynamic cryptogram that is transmitted via the CVV2 field, and use either a Token PAN or original PAN with the EXP Date as a Token Mode Indicator, then authenticating the dynamic CVV2 cryptogram. Together, this provides issuers with scalable tokenization security and consumers with the best user experience to start changing their habits from cash and plastic to mobile authenticated payments.

As you'll see in the coming years the proliferation of devices will continue to grow and what we call token delivery devices will expand beyond smartphones and into wearables, Internet of things, and even accessories that hang off your keychains. Our job is to make sure that we as a token requestor and a secure container can properly store those tokens and deliver them for the consumers to as many places as possible and as many end points as possible.