Devaluing Data: If the System Cannot Be Made Secure, Can the Information Be Made Worthless?

Moderator: Marianne Crowe

Ms. Crowe: Among the motivations for this conference are incessant cyberattacks and large-scale data breaches that expose millions of consumers' sensitive information and billions of dollars of fraudulent payment transactions. The previous session illuminated that even with the various security standards, protocols and procedures in place, the vulnerabilities to data security persist. And in response to merchants becoming more PCI compliant, hackers have moved on and now are focusing on exposing data in transit by inserting malware into merchant point-of-sale systems that then takes the clear text data as it moves and ships it to the hackers' databases instead. Then they are attacking the data instead of doing it at rest in the merchant databases and networks. Through such occurrences, we have come to understand that while a merchant may be declared PCI compliant at a point in time, as was said earlier, there are still unknown holes and missed patches and other gaps that can invalidate that. The migration to EMV chip in the United States is going to protect card data from being used to duplicate the physical card, but, as we know, it is not going to stop hackers from stealing EMV card data as it travels through merchant systems if it is not encrypted. Hackers can still expose this data and then sell it for use in making fraudulent card-not-present transactions, for example, in the growing e-commerce space, as was discussed in the earlier panel. During this panel, we are going to discuss technology alternatives to better secure and devalue data. I am very happy to have four really great experts in both the payment and security field on the panel this afternoon: Steve Schmalz, Radha Suvarna, Madhu Vasu and Branden Williams.

To begin our discussion, I want to frame the task by stating how payments data security has been viewed to this point. One ideology was to build a better wall to protect the data, and I think it can be argued that much of what we have been doing has been building these higher walls.

PCI compliance, for example, falls into this category. There has been a lot of success on this front, but as we know and as we have heard, it is not perfect and criminals keep figuring out ways to breach those walls and find new ways to get into the system. There is no one solution to the security problem. Instead, we need a multilevel approach to data security and fraud detection as a strong defense. And it appears that momentum for building such an approach is starting to happen, and it is relating to how we can devalue this data and make it useless, which is the topic of this session.

In applying the devalue-the-data model, card networks, issuers, processors and merchants are employing security technology so that cardholder data is stopped before reaching the point-of-sale systems and is rendered useless, even if it is exposed to fraudsters. This three-pronged holistic approach envisions EMV chip, tokenization and point-to-point encryption working together to protect payment data from the beginning of the payment transaction through to the end. With that as an overview, I am going to ask each panelist to take five minutes to share perspectives from their organizations and what they are doing or planning to do to devalue the data. We are going to start with Steve Schmalz.

Mr. Schmalz: I want to talk about the work that is being done at X9 F6 on a new tokenization standard. Rather than talk about that particular standard, I want to discuss what, to me, has been an evolving understanding of what is tokenization. I hear the word thrown about. I hear terms like, "Use tokenization to protect the network," "Use tokenization to protect the data at rest," etc. Token has become an overloaded term. It might be helpful if I talk about what the group has decided to use as a way of defining categorized tokenizations within a payment card system. Before I do that, I want to try some comic relief.

Are any of you fans of "Red Dwarf"? It is an older show out of the U.K. But it is a great show, and there was an episode … I have to set this up. There is a cat, a robot, a hologram and a human on a spaceship, and they probably are the last living things, millions of years in the future. And they are wandering around and they go through this portal and they end up a million years in the past. And the cat turns to the robot and says, "Well, what just happened? What is it?" And the robot says, "Oh, it is a rip in time. It has allowed us to move across the spatial continuum." And the cat goes, "Oh, thanks." It turns to the hologram and says, "What is it?" He says, "It is like a black hole that allows us to move through space and time." It turns to Lister, the human, and says, "What is it?" And Lister says, "It is a magic door." And the cat goes, "Oh, well why didn't you say so in the first place?" I tend to think that sometimes when I hear the term "tokenization" thrown out, it is thrown out as a magic door. It sort of automatically protects everything. So I want to try to put things in context. The tokenization standard that X9 F6 is working on focuses on what you might have heard of as a security token, whereas the EMVCo framework talks about payment tokens. Well, those terms are sort of accurate, but they also create a bit of confusion. Let me give you some background on the "security tokens."

You probably all know that PCI gives you relief of some of the auditing requirements if you use tokenization. Where the tokens live, the token is supposed to be worthless, so you do not have to actually focus any effort in seeing whether or not there is any potential loss of data there. The tokens are supposed to be worthless to an attacker. And the reason for that is the credit card number comes in, bounces through the payments system, and goes from merchant to acquirer, usually at the acquirer it gets turned into a token, and then when the information comes back, rather than having the credit card number stored in repositories, the token is stored in the repository. That token, sitting in that repository, has a lot less value than the credit card number, and arguably it may have less value than an encrypted credit card number because encryption usually involves some type of key management, and you have to make sure that the key management is not exposing keys, which brings the auditors back in. That more or less is the birth of tokenization as a security mechanism.

Now with EMVCo, a token is created before the payment transaction takes place, and when the payment transaction takes place the token is actually provided at the initial point of sale. It may not be provided in a point-of-sale device, but initially the token is given over instead of a credit card number. And then the token works its way up. At the top, at the issuer or the bank, it gets turned back into the credit card number and then some type of information comes back down to allow settlement after the fact. What is the difference? They both are tokens, but why do they use the term payment token in one case, and security token in the other? You can argue, well it is a payment token because it can be used just like a credit card. True, but it gets converted back to the PAN (primary account number) in the back end to finalize the settlement, and then you can argue that the security token is still part of the payment process. I think a much better way of looking at this is to use terms that the industry uses, and that we now use in our standard, and that is not to call it payment or security, but to call it a pre-authorization versus a post-authorization token. That makes things pretty simple. Well, maybe not simple, but maybe it clarifies them. The term post-authorization simply means the token does not get created until after the PAN enters the system. The PAN is put in a point-of-sale device. As I described before, it bounces from merchant to acquirer, issuer/bank, etc. Somewhere along that process it gets turned into a token, and then when information comes back and you need to store what in the past would have been the PAN, you can store the token instead. So, the token is a pointer that allows you to get the PAN back when you need to. It sort of fills the void. It sits there and represents the PAN, but it happens post-authorization. The transaction gets authorized first before the token is created.

Pre-authorization simply means the token can be used to fire off the payment transaction. As such, it looks a lot like a credit card number, like a PAN, but is different in the sense that it can only be used in a limited scenario. It can only be used on certain mobile transactions or to maybe charge certain types of objects, etc. That pre-authorization token cannot be used at your local department store to buy something. You cannot swipe your payment token. You cannot swipe your pre-authorization token.

Calling it pre-authorization and post-authorization, I think, helps clarify what role the tokens are playing, and our standard focus is on post-authorization tokens. Now, that is the difference. There is a similarity in the sense that they do both provide security. Obviously, the post-authorization token is primarily a security mechanism. It is aimed at doing that. It gives very good security, but in a limited framework. It does not provide security for the whole payment process. It provides security after the initial authorization takes place. The pre-authorization token provides security, but it does it at a cost in the sense that the pre-authorization token can be used to charge things. So what happens in EMVCo's case, you do not just send the pre-authorization token, you send the pre-authorization token with some type of cryptogram. I am not going to go into the details, but there is a way to secure it, to make sure a hacker cannot use it on its own. You have to have access to multiple mechanisms to produce this package containing the token to actually charge something with that pre-authorization token. So in one case, you have purely a security function with post-authorization that is a little limited, limited to after-the-fact storage, etc. You have to put additional security mechanisms on the pre-authorization token, but it gives you more security across a wider swath of the payment authorization piece.

Hopefully that was not too confusing. You may be hoping that I had just described a magic door. But I think maybe it will help you keep things in context. When you hear people say, “Why not just use tokenization,” that is a very vague term. The last thing I wanted to say involved what you might consider doing. I had a math professor who said a “Change of variables is good for the soul.” If you have ever taken a math course, you may understand. I would not worry about it, but the next time you hear somebody say tokenization, think: “Why not call it a funky crypto-object and tell me what you are actually doing with it. Tell me the protocol, tell me the system it is in; tell me how it is being used. Do not just throw out the word tokenization. Tell me what is going on.” And that is a far more educational experience than just using the magic door.

Mr. Suvarna: Just 30 seconds of background on what I do, to give context to my view. I head up emerging payments for the credit card business; basically driving this strategy of mobile payments and driving partnerships with networks and technology companies, industry players and wallet providers, bringing solutions to the consumers, and launching those solutions and driving usage and adoption. In that sense, my team’s responsibility is more on the business side. My comments and my views are probably more from a consumer and business perspective, and I might twist and tweak the technical definition of token.

From the perspectives of businesses, consumers, banks and the ecosystem, security clearly is important for a number of reasons and a couple of reasons most importantly. One is the adoption of mobile payments, or at least the evolution of mobile payments. For us to get consumers to adopt some of these new solutions, we have to get them comfortable and say, “Hey, use these, these are as secure if not more secure.” Because it is new, we need to step up and help consumers understand. Security becomes an important function there. The second is all the breaches. For those two reasons, we as an ecosystem and as a bank need to start thinking about security in a different light. The good thing is, as Marianne Crowe stated, there are now tools available—EMV, tokenization and point-to-point encryption—that we can start using to drive better value and enhance the security of the payment ecosystem. As Liz Garner mentioned earlier, there is no silver bullet. But put together, we can start to deliver a better, more secure solution for consumers. And without going into too much detail, I think the simplest way is EMV, securing the plastic and helping to reduce card-present transactions fraud; that may solve a set of problems. But it does not do enough to address the card-not-present transactions, for example. That is where tokenization comes into the picture and says, OK, how can you make the information less useful?

If you replace the actual card number with the token, suddenly we are saying that is more secure, and you might wonder why. You still are using the token to make the transaction. Why is it somehow more secure? I think the fundamental paradigm that I look at, and I start explaining to my executives, who obviously do not have time for understanding technology, is hey, here we have a 16-digit card number that is already powerful. If somebody can get access to that number, they can put it on a mag stripe and make transactions. They can go online and make transactions. They can do a bunch of different things. What if we could come up with another paradigm that basically says, you create a token and identify it for a particular wallet solution? As an example, Apple Pay. Or, you create another iteration of that same card number for a particular merchant, merchant XYZ. If that information is stored, customers can use it only to conduct transactions in that particular context because when that authorization comes in, say this token is coming in, it is assured for this particular wallet, but it is coming from this merchant or plastic, wait, something is wrong. Decline it. So, it is not making the chance for fraud zero, but it is reducing it; fundamentally, that is what tokenization does. Of course, you overlay EMV and point-to-point encryption and then it starts to become much more powerful. That is the very fundamental level of what tokenization is because it is a contextual number, changing the pattern from the all too powerful 16, 15, whatever digit, card number.

Now, from a banking perspective, getting and adopting some of these solutions and doing the security has value for the entire ecosystem because it reduces the disruption for consumers. It drives innovation and reduces fraud, which has a cost to the system. The last point I would make is that it is not going to happen automatically. We as an ecosystem and industry need to come together to drive standards around consistency of user experience. By putting consumers at the center—all of this technical talk is going to make sense for those of us who are students of this space—but at the end of the day for the consumer, it has to be simple. That is what we have to figure out, and that is what is going to drive ubiquity and adoption and actually solve the problem beyond the technology that it is today. I am looking forward to more discussion on that.

Ms. Vasu: I am privileged to be part of this panel. I am with the innovation and strategic partnerships at Visa. Since Radha and Steve covered a lot about tokenization and the standards, I am going to take a different twist and talk a little bit about my personal experience with disintermediation. We talked about new form factors in the payment landscape—evolving, changing the ubiquity of mobile devices.

An example that hit pretty close to home for me was I had the Starbucks application on my mobile device, and I was walking with a co-worker to the Starbucks in Foster City, Calif. I had the QR code, so basically what the Starbucks application does is it takes your payment credential, your 16-digit PAN, and it has what is known as a token, which is a QR code. But that token is basically just a mapping between the PAN in the back end. So my co-worker said, "You know, how secure is this?" And I said, "This is really secure." This was about three years ago. So we did not get into tokenization, there were no standards or any of that at that point. So he said, "I am going to take a picture from my smartphone of your QR code and buy you coffee today." And I said, "There is no way that is going to work." But my worst fears came true when he was able to use his smartphone to take a picture of my QR code on my application and scan my QR code from his phone at a Starbucks counter … and it worked. And my payment credential was being debited. That was a typical example where a payment credential was being passed through a different form factor, through different channels, and it can be compromised. The security of the payment credential was at risk.

Another example would be something like Google Wallet, where you have a MasterCard that is being front-ended. As a consumer, I think I have a Visa card in my Google Wallet and I think I am paying with a Visa card, and it is a card-present transaction because I go into a store and I use the Google Wallet. But what is happening is Google is basically front-ending my Visa card with a prepaid card. They submit the transaction to the issuer as a card-not-present transaction because they acquire the first transaction, which is actually a card-present transaction. I get an SMS on my device giving a different number from what I have in the Google Wallet, so there is consumer confusion. In the case of returns, I have no idea what the merchant actually saw. I think it is a card present, but the merchant sees a different credential. In case of disputes, the issuer sees a card-not-present transaction while I think it is a card-present transaction. Basically, as a result of all these form factors, there is disintermediation and confusion about chargeback rights. With respect to the tokenization standard, the EMVCo specification was put into place, and Visa's part in that was we came up with what is known as a "token service." We are working with the token requesters like Apple, Google, Samsung and other digital wallet providers, and there are certain key tenets that I want to drive home as part of this discussion.

When a token gets created, it gets provisioned on to a mobile digital wallet like Apple Pay. As part of the provisioning, the issuing banks are participating in what is known as an ID&V process, the Identification and Verification process. In some of the earlier discussions, there were talks about why is it that we cannot use the device ID, why we cannot use geolocation, IP addresses of the device to make sure our risk decisioning is more secure? That is exactly what we are doing from an ID&V process. So, before the token gets provisioned, it basically is going through a risk assessment using these new nonstandard data. As a result, a determination is made whether a token needs to get provisioned or if a consumer needs to be subjected to additional authentication. They might have to receive a one-time passcode or call a call center and authenticate themselves again, or log into a mobile banking application and re-authenticate themselves. So that is the identification as far as provisioning.

The second component is transaction processing. During transaction processing, the token that gets transmitted during a purchase, when it hits our network there are certain domain restriction controls. Radha talked about domain restriction controls where the token is intended for just one particular channel, domain, or merchant. So those restrictions come in. That, combined with EMVCo cryptograms, makes a tokenized transaction more secure. It devalues the underlying data. Even if the token is compromised and used in a card-not-present transaction, it would not get authorized.

Mr. B. Williams: We have a lot of token talk right now. It has been interesting, but my experience at First Data, especially recently, where we have initiatives going on where we have a token of a token, or a token of a token of a token, feels like we are in the movie "Inception." We are going down multiple levels of this thing. I think tokenization has turned into this year's version of big data or cloud or virtualization, where people do not necessarily know what it means or know what it means to them. Frankly, I think a lot of people are afraid to ask the questions. So what I always tell people is do not leave a meeting until you really understand exactly what you are talking about, much to Steve's point. Get down to the nitty-gritty details. Make that person explain it to you.

In the case of First Data, what we are talking about, is devaluing data right at the merchant; we think that probably is the right place to do it. We sort of have this end-to-end approach. We pull right from the swipe, and we devalue the card number there and replace it with a token on the way back down. At this point, the merchant and anybody in between, it could be a gateway or it could be somebody else, really cannot see that data. It is devalued in their perspective where it is just a stream of information that does not make sense to them and what they get back is a replacement value that they can use for a number of different things, like chargeback, settlement, or clearing. Anything else like issuer loyalty and things of that nature.

Our goal is to really solve the bigger problem. I have done a lot of work in the PCI space. I think in the last five years, we have gotten to this point where the industry is marching along to the beat of the PCI drum, and nobody has stopped to ask why we are still doing this, does this really make sense, are we solving the problems that we need to be solving, aside from trying to reduce PCI scope by deploying technologies like this. With encryption keys, when we talk about protecting data in motion, there are a couple of ways it can be done. Asymmetric encryption is what we do for online types of transactions and symmetric encryption is where I have the same key to decrypt and encrypt. Symmetric encryption is typically a lot quicker; asymmetric is typically slower. But there are benefits to asymmetric encryption. In fact, we would not have online commerce without asymmetric encryption. So, they can be used to encrypt the same or different types of data, but the point is that it cannot be read.

Looking at tokenization technologies, the difference here is that encryption is what protects data as it is moving, tokenization is what is effectively going to protect it while it is sitting in the drive, sitting at rest. We strive to do everything possible with that payment transaction with the token after that token has been issued. From our perspective, what we call a token is a replacement value for the PAN. It is the same 16-digit, 15-digit number. In some cases, parts of it can be preserved so right at the terminal when the receipt prints it will say the last four digits so the consumer does not get confused in looking at the last four on the receipt. And we have had instances where merchants have had terminals go missing, been stolen, and this is before the settlement was batched for the day, and there was no card data inside of that terminal because it was all tokens. There was nothing that anybody really could do for a merchant.

Tokenization has another issue with single use or multiuse. In the case of a recurring charge, some of the tokens have to be able to be used, be presented for a reauthorization in the next month. So, there is another nuance in different types of tokens that you see.

Ms. Crowe: Since we are on the topic of tokenization, we will stick with that for a little bit. But I did want to go back to Branden for a second, and then the others can jump in. Since we are talking about multilevel security and you mentioned encryption, how do Visa and Citi feel about the combination? Where do you see the value added, encrypting and tokenizing the PAN?

Mr. B. Williams: You can do one without the other, but I do not think anybody can get the value with one without the other. We talk about layered security. Or defense in-depth. Static defenses are not what we need; we need dynamic defenses, because static defenses can be compromised because you learn how the system works. And we did not solve for the math problem of elliptical curve. We just walked around the encryption key and got what we wanted. From our perspective, we can deploy one without the other; I do not know why you would. I mean, if you are looking to really solve the issue, which is to truly devalue the data as it moves not only through your system, but comes back and stays resident in your system, then you have to do both.

Mr. Suvarna: I think the simple answer is both of them will work together, and they are not alternatives. They are complementary solutions. Like I said, without understanding the depths of technology at the very simplest level, even the tokenization from merchant to acquirer, acquirer to token wallet, whatever it is, if it is starting with the network, the token wallet, the token is traveling, but from network to issuer in some parts of the transaction leg, the card information is still transmitted between points. So, at that point, if that needs to be secured as well, I am guessing point-to-point encryption is needed. So, at a basic level, I do not necessarily see them as competing alternatives, they are complementary solutions.

Ms. Crowe: One question that came up is if in fact it ends up being tokenized at the beginning, through the payment, all the way to the end, the pre-authorization and the post-authorization, and you go through all that process tokenized, does it down the road, maybe not right away but in the next few years, make the need for encryption go away?

Mr. Schmalz: No. First we are using the term encryption. I would like to use the term cryptographic mechanism because you can do a lot with cryptography other than just encrypt something. You can digitally sign something. So you can protect not only its confidentiality, the value of it, you can protect its integrity and you can do repudiation, and you can make sure people do not change it, and you can lock something in so they can only use a certain piece of that in a certain way. So when I say no, so you are talking about the EMVCo, what I call the pre-authorization token, that token is only secure because it does not get sent by itself. It gets sent with cryptograms, which in essence are cryptographic mechanisms used to tie the token to the transaction and to make sure it cannot be used in any other context. I do not want to go into the details of the actual cryptographic mechanisms. So that is the first thing.

The second thing is at some point in the back end, it gets turned back into a PAN, and back there, I am hoping, it is not something I know a lot about, but I am hoping there is some cryptographic mechanism that is used to protect it. That may or may not be the case. So you have to think of systems here. Sort of back to what I was trying to get to before, to separate out tokenization from other cryptographic mechanisms and to isolate one and think that tokenization will give you all the security you need, that is a pipe dream. You have to combine other methodologies with it. In the case of post-authorization, the PAN travels in the clear without encryption. First Data, Heartland, they all do the same thing in the sense that they secure it when they get it between when it comes into the system and when it gets turned into a token. So you cannot separate the two. You have to look at it as a system; you have to look at the total protocol.

Ms. Vasu: I would like to add to what Steve just said. I do not think it is a one fits all solution for everybody. A hybrid solution based on the need that we have is very important. So a combination of encryption with tokenization and with also, for our merchant friends here, what we have is the payment account reference, the PAR, because they actually need the PAN back for loyalty programs, for fraud and risk, and this is something if we send in the clear today defeats the purpose of tokenization. So, we are working on the PAR, which basically gives the ability to tie the payment credential across multiple token requesters. It would be a combination of all of these technologies that would basically benefit, and I think isolating one from the other would not be very prudent.

Mr. Schmalz: The PAR is an interesting situation. The next time you hear anybody throw out the term tokenization as the end all/be all of security, without any differentiation, think about the PAR, because there is no need for PAR in the post-authorization token if you need the PAN back, you have access to detokenization services. In the post-authorization scenario, in fact, you probably do not want to give any detokenization functionality to anybody until the very top of the payment chain. But what does that mean? There are going to be multiple post-authorization tokens living in that system, and you as playing your part in the payment processing work flow, might not need to know what the PAN is, but whether it is the same PAN being sent. In fact, there may be anti-money laundering requirements. So what are you going to do? Well, you have to have a mechanism like this. Here is an example where one size does not fit all. You need different security mechanisms, different pieces of data, to make them both work. That all being said, I know that Liz Garner mentioned that might be an issue from a security standpoint in ways that it might disclose information to others in the system. I am not trying to start a controversy. Actually, it would be fun if you guys had a discussion on that. But it is just something that you need to think about. It gets complicated. Even what looks like a simple solution gets complicated.

Mr. B. Williams: Why not take a real world example. For those of you who have Apple Pay, say you have been shopping at a merchant with your credit card for years. And now, the next time you go, you use your phone and you pay with Apple Pay. The merchant does not have the original PAN anymore. They have the EMV token that is your Apple Pay enrollment, so they cannot tie your new purchases to your old ones, just like Liz was talking about how you cannot pay with a credit card and refund with Apple Pay. So there is a situation right there where we have two different tokens or two different representations of the same individual. That is in one merchant. So the PAR is a different scenario where we can go across multiple merchants, we have anti-money laundering, loyalty, other things. We were just talking about at the coffee shop.

Ms. Crowe: Well, we can continue that with the Q&A afterward. But still talking about tokens and if tokens basically secure the payment credentials, we know the token service provider, whether it is one of the large issuers or the card networks for now, are storing the original PAN and doing the mapping when it is needed to be passed around the process. So what kinds of security, for someone who might not understand that, is in place to make sure the token vault itself is secure? Start with Radha and then Madhu.

Mr. Suvarna: I would probably pass it on to Madhu. We do not have a token vault. We do not have this service.

Ms. Vasu: From a network perspective, it is sitting in a place behind our company's firewall, of course, and it is as protected as our authorization systems today so it is in a highly secure zone. The keys required for detokenization, applying the domain control restrictions and validating the cryptogram, currently exist within the network because it is a network token solution. So the token service provider is the only one who has the ability to do this. There is a key exchange with the issuers in some scenarios, but pretty much the vault is the system of record.

Mr. Suvarna: Even though we do not have a solution, from an issuer perspective, the card credentials are issued by us, and they are already in our system. So tokenization does not increase the risk anyway, it is just the mapping. I am just clarifying. Tokenization, having a token work does not necessarily increase the risk. It is already there.

Ms. Crowe: So if I were Amazon or PayPal or some proprietary organization like PayPal, they have their own token vault for their back end or post-authorization tokens. Would they say the same thing, that is how they are protecting the security of their tokens in their vaults? Because they consider themselves token service providers for their own merchant customers.

Mr. Schmalz: Back in my QSA (Qualified Security Assessor) days, I helped a couple of different companies build something like that because there was nothing available. They built their own token solutions internally. I think what we are finding is that token solution still internally, it turns them into a bank or something that they are now having to protect, and a lot of retailers, frankly, do not take the same level of security that a bank or another financial institution would.

If I could give a quick plug to the F6 tokenization standard, those are exactly some of the issues that we address. We talk about how to secure what is called the tokenization service, which includes that vault. And we talk about how to securely talk to it, how to the secure communication, the authentication and authorization, the ability to ask for a token or detokenization services, etc. It is also important to point out that what the solution looks like depends on what the actual tokenization mechanism is, what the algorithm, for lack of a better term, is on the back end. Because there are multiple ways to do this. Initially the idea was that you had to randomly produce a token every time you saw a PAN, and that is how you produced this unique one-to-one matching. But the industry determined very quickly that it was just as secure to do something like 256-bit keyed AES (Advanced Encryption Standard) where you use format preserving encryption, but you only do it in one place, and you take that 256-bit key and you stick it in an HSM (hardware security module) that is some 140-2 Level 3. So the mechanism you use to protect it is different depending on the algorithm you used on the back end. But what is important, and this is very important to me, is that what makes the post-authorization tokenization "tokenization" as opposed to encryption is the fact that it only happens in one or two spots, that there is a service where you have a lot of security protecting it, where you have to go to get tokens or to get PANs back for tokens. And so securing that is key to everything. If you do not do that, you do not have a secure system.

Ms. Crowe: I want to shift the conversation a bit, but stay on the tokenization theme; Apple Pay, Samsung Pay, I want to have secure elements in the phone that store the token rather than the PAN. And so we know that secure elements are considered, you always say tamper-resistant or tamper-proof, right? But then we have Google Wallet, which was mentioned earlier, or Android Pay, which I understand will use some type of tokenization, but they do not have a secure element; host card emulation and the cloud are involved. So can you explain how that is going to work?

Ms. Vasu: With Apple Pay it was a secure element implementation. And with the Android ecosystem, it is highly fragmented. In the case of Apple Pay, Apple owned the device, the operating system (OS) and they had full control over the real estate on the device. Whereas, with Android Pay, Google has more than 300 original equipment manufacturer partners. They have different partners who have control over the real estate, and to provision it on to the secure element is literally a struggle. So the shift in the industry was to move to a host card emulation where the token was provisioned in the cloud. But there are some security concerns as far as provisioning and keeping the credentials in the cloud. So even though it is a static token, the implementation model uses what is known as a limited use key. The limited use key is dynamic in nature, and it has certain parameters or thresholds like the number of transactions, the transaction amount, the usage, etc. So once these thresholds are reached, the token becomes invalid, until a new limited use key is sent back to the device. The token with the limited use key resides in the reloadable memory of the device, and that is how it gets protected, and that is how it is different from a secure element implementation.

Mr. Suvarna: I think that is an accurate description. Just looking at it from a slightly different angle, what we as an ecosystem will have to figure out is, one victory is obviously making it as secure as you possibly can; another is looking at how you can come up with a solution that is ubiquitous, drives consistency and gives you the value. I am not contradicting anything Madhu is saying. I am just adding. By going with the host card emulation, and it may not be as secure as secure element, but many more phones in the industry can become ready for tokenized solutions, and more consumers are walking around with more secure solutions than they otherwise would have had. The net impact is that we are as an ecosystem more secure. I think we also need to collectively focus on how we are going to keep it simple for the consumer. We are just having to figure it out as space is evolving. We do not want to make consumers do too much work because they are not going to adopt. This could be a great technology, but without consumer adoption it is not going to be of much use. So we have to figure those things out. That is where standards come in, not just the technology standards, the specs and the likes, but also the decisions we are making to keep it simple for the consumers while ensuring every ecosystem's needs are being addressed whether it is merchants, networks, banks, issuers or wallet providers, to continue driving innovation. We just have to figure that out. I think the industry is making good progress. We just need to always have both lenses on, that innovation is not completely focused on making it as secure as possible, but you also have to have what is going to make it more ubiquitous and adoptable so we can have the right combination of the net effect.

Ms. Crowe: And that may mean a compromise between different stakeholders in terms of how and what standards get put out. So one question before we turn it over to the audience. We talked a lot today also about card-not-present and e-commerce transactions from a tokenization standpoint, but also the two other prongs of this devaluing the data in e-commerce. So for in-app and e-commerce, how do you see particularly tokenization playing a role? We talked about 3D Secure, but what about tokenization? Is that going to play a role?

Mr. B. Williams: It can play a role. It plays a role today. EMV tokens are what Apple Pay is, so it already plays a role. But I think that there is an opportunity for companies who have mobile apps to use tokens provided by their acquirer, store those tokens on the mobile device to be submitted for payment, as opposed to the actual card number. There are tons and tons of options in how it could be used and deployed. Whether that actually solves the problem or not I think is a really good question. We should look and see, does this actually solve the problem by adding all these tokens and adding all this additional stuff. I think it probably does, but we should probably look.

Ms. Crowe: Is Visa doing anything with it?

Ms. Vasu: We are using a TAVV, a Token Authentication Verification Value for in-app, e-comm transactions. However, I think liability will be the next question to come up. So we have not made any changes to the liability because we are still in this mode where we are analyzing and assessing, because for us to effect a liability change, we need to make sure that there is issuer authentication at the time of the transaction. In the case of Verified by Visa, like 3D Secure, there is a password and a consumer types in a password to authenticate themselves that the issuer authenticates. But in the case of an in-app, that does not occur. So you do have a cryptogram with the associated token, but currently Visa's stance is we are evaluating and we have not made any changes to the liability.

Mr. Schmalz: The only comment I would make is tokenization does play a major role in the sense that you do not have to put the PAN on the card-not-present device. You can put a token instead, which I am just echoing what everybody said here. In addition, there is one last point I would like to make. These tokenization systems are systems, and whether it is card-not-present or any other payment system, you cannot forget that there are other things you can do to secure it other than just the controls of encryption, tokenization, authentication and access control. You can monitor, you can look for fraud. We have heard about that today. You have heard from the Department of Homeland Security, and everything that was said there was about monitoring transactions, put it in the language of payment, monitoring the transaction and looking for something funky happening. And that technology is just as important to deploy. So the name of this panel is if systems cannot be made secure, can the information be made worthless? Well, the answer to can the information be made worthless? Almost, but not quite. If the system cannot be made secure you better be trying to make it as secure as possible. So you need to hit both sides, and "try and make it as secure as possible" means multiple other security mechanisms need to be put in play.

Mr. Suvarna: I would only add to your question about should e-commerce and others be addressed through tokenization, and the answer is absolutely yes. I would go back to the same thing. Tokenization is a great technology, but the application effort, if it stays with mobile wallets and so forth where there is 0.01 percent of the transactions—I do not even know if it is that high—it is a great technology, solves the problem, but it is applied to 0.01 percent of the volume, what good is it? So obviously, we have to go and address and apply this cool technology and solution to where the volumes are, where we can actually get some benefits in the ecosystem. It is not a question of should we; we absolutely have to. The question is, how are we going to get there, and what sort of standards? For the right reasons, the ecosystem has started with the mobile wallets and so forth because that is where it is easy to implement a solution now that we know how it works and there are kinks and we will figure it out. That is when we say OK, this is good, it seems to work. So now how can we take this and apply it somewhere else? That has to be the game plan.