

General Discussion

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

Mr. Santhana: I have two questions. First one for the pre-op group, and the second one for the post-op group. For the pre-op group: Gemalto announced last October at the Money20/20 conference that they are about two to three years away in creating chip cards where the issuer can provision tokens at the point of sale. Have you had conversations with card issuers to see when that could be implemented, accelerated? I am talking about network tokens, NFC (near field communication) cards. In terms of your discussions with card issuers, do you see how that could be implemented?

Mr. Suvarna: Yes, in our case we are the card issuer. That definitely is an interesting idea. Honestly, from an issuer perspective, the way I look at it is there are digital wallets that are new, and then there is e-commerce that does a lot of volume, and then there are plastics where there is a heck of a lot more volume. So we have started with digital wallets. The next step is where do we go next, e-commerce or plastics? It is a matter of phasing in a new solution. Logically, it makes sense. Once we solve the e-commerce problem, then the question is, now that we have plugged those two holes, should we apply the same thing to plastics and does it make sense? And logically speaking, it seems to make sense. If there is a technology to figure out how you would put a token inside the chip of an EMV card that is different from what is embossed on the card, that sounds like the right thing to do, right? So I think it is a matter of evolution. There are other things to solve right now, and I think industry will eventually get there. It seems like the right thing to do eventually.

Mr. Santhana: But my question was will you be there in two years when Gemalto is ready?

Mr. Suvarna: Honestly, I would say in the space I am in, emerging payments and technology, two years is a long time. I cannot even predict what is going to happen in six months. So maybe; maybe sooner. Who knows?

Ms. Vasu: I agree with everything Radha said. And from a network perspective, if it is going to have the same format as a token on a mobile device, I do not see why we cannot support it and why the other ecosystem players cannot support it. It is just a question of will we start seeing those cards with the token on it that can be used in different form factors and also can be used to dip at a terminal.

Mr. B. Williams: Can I disagree? Panels are more fun when people disagree, right? So that form factor that you are talking about has existed in some form for a long time. I worked at Verisign prior to my time at EMC and we had one. So the question was, does this not solve a lot of problems? You have an algorithm right there, you can emboss a card number on it, they can hit a button, they can get a two-factor there, or we can just do tokens and issue tokens. You know, you have one vendor driving it in an ecosystem that may not be quite ready for it. We have to think about things like backwards compatibility. So, look at Apple Pay again. It is a backwards compatibility issue. The token is a 16-digit number, but it is a routable number. So while the issuer, Citi, gets a second set of BINs—they have their Apple Pay BINs and they have their regular BINs—we still have to think about that acceptance problem and how we get people using it. EMV is a perfect case study for how long it has taken us to get it and how in a lot of cases small merchants are almost being left behind.

Mr. Schmalz: If I could ask a question. So is the token being generated on the chip or is it being requested by the chip from some ...

Mr. Santhana: Requested by the chip at the point of sale.

Mr. Schmalz: So, you are just having a point-of-sale device make the request for tokenization or detokenization services directly and that is an infrastructure issue. Yes, that is fine. Then the tokens produced should be a token that is routable. So yes, there is nothing wrong with that. By the way, I would not call it a network token. It is a token.

Mr. Santhana: Maybe I should use “pre-op” versus “post-op.” So for the post-op question, the problem I see on the post-op side is now you are dependent on the merchant to provide tamper-resistant terminals and point-to-point encryption because the issue with tokenizing after the card information is captured by the device, at some point down the chain, is you are now dependent on the merchant implementing tamper-resistant terminals.

Mr. Schmalz: Yes, and you had the problem before, but you also had the additional problem of what do you do with the primary account numbers (PANs) when they come back. How do you store them securely? So you are

talking about an issue that is solved with chip and PIN cards, and you are talking about an issue that has been around for a while.

Mr. B. Williams: And by the way, we do that today. You do not qualify to get the tokenization encryption unless you have a modern terminal, which is going to meet all those requirements.

Mr. Moore: I would like to hear more of your thoughts on online and e-commerce applications. Forget mobile for now because it is 0.01 percent if we are lucky. And if I am entering my credit card number in my browser, I have this insecure computer that could have malware on it that could observe the card number, and then there is the potential storing of that card number at the merchants. There are lots of places where we have to share our card number in ways that could be compromised. Can you discuss what efforts, if any, are being considered in trying to devalue that card number and its use on computers and also on the merchant back-end networks?

Mr. Schmalz: That is an interesting question. What you are saying is if the computer is compromised, how do I prevent somebody from sniffing a credit card number, a PAN I just put on it? If you put the PAN on it, you cannot. Can you do something before you put the PAN on it? Yes, I guess you could produce a token that is not valuable before, but you would have to intervene. I just want to understand the question better. It seemed like a question where there was no good answer.

Mr. B. Williams: Unfortunately we cannot protect the consumer who has malware on their machine. They have to participate in their own rescue. They have to put their own tools on there to do their own things, and they do not want to do that because it is so much easier to just to hit “Buy Now” on Amazon; one-click buy. But then you talk about if the consumer is compromised and fraud is on that card. That smells to me like an issuer problem. The issuer is the one who probably would take the liability if there is no common point of purchase where they can sort of push it down the chain. You guys can correct me if I am wrong, but that is what it smells like to me, is that it is an issuer issue at that point. So then issuers today, they have fraud tools. If you bank with a major bank, you probably have had your card shut down at a very inconvenient time because they are “doing you a favor.” So, it happens. They are protecting their losses based on what they have. To me it is like two separate issues.

Ms. Vasu: Yes, there are a couple of things I would like to add. If it is malware on the computer itself, then there is nothing much we can do. We are in discussions with several companies in the browser business, and they

are actively looking at using tokenization, with the least impact to them. If they now have to enter a token instead of a PAN, they are going to have to redesign a lot of their Web pages and input different criteria, which is a huge effort. Some of the discussions in the industry right now are about keeping the same merchant website intact, but in the back end, we ensure that those websites are token-enabled. So there is a token that gets sent once the consumer enters this data. The concept of applying the token throughout the acceptance environment in the network to the issuer would still apply at that point. The question here is there are no standards, it is in the very early nascent stages, but we are having those discussions. That is just one part to solve for browser-based e-commerce.

Mr. Schmalz: There is one other point I think might be important to make. There is technology today where you can download JSP (JavaServer Pages) to a browser, which has the capability of basically taking a snapshot of the system and monitoring. We can notice when something changes, when it looks like your computer might be infected. So rather than say what do you do when a computer is infected with malware, to protect the data going in, you can say can you detect or have a chance of detecting endpoints that have malware on them and then alert the owner or refuse to accept online transactions from those computers. So there absolutely is a way; you might not want to support that as a company deploying these solutions, but I know from an authentication standpoint there is a way to download JSP, which basically takes a fingerprint of the device and can see things happening that might indicate if the device has been compromised.

Mr. B. Williams: I want to add to that because I think that is not a great solution for a couple of reasons. First, a merchant is never going to say, “No I am not going to accept this transaction.” Merchants always accept the transaction unless someone tells them not to. Second, with that type of solution, you have created another antivirus blocker. I have to know what to look for to determine that something is wrong. If I have never seen it before, or seen behavior like that before, I might not actually know what to look for. The cleanest way that I have seen it done is very clunky for the end-user, but having disposable virtual machines that are downloaded on the machine one at a time. That is not going to solve for keyloggers, and does not solve for other things, but it does allow you to add some of that dynamic stuff where it is a one-use piece. But I like where you are going. I think there is some interesting stuff there. It is a bigger issue, bigger than payments, this problem of browser security and drive-by downloads and things.

Mr. Schmalz: Branden, that is a great point and it brings up that you need to balance your security mechanisms with the cost. It is always a

balancing act, and there are difficult decisions. It may be that you actually put up with a little bit of fraud because that is the cheapest way of keeping the business up and running and profitable.

Ms. Zhang: My question is related to software-based security. You mentioned that the HCE-based wallet is a software base. Compare that with a secure element-based wallet, Apple Pay-based, you go through some certification of the hardware. My question is when you implement these HCE-based, maybe this is for Visa and other network vendors, do you do any certification on how they manage the token and the keys in the user devices, make sure they implement it correctly? Especially you talk about the different platforms for Androids.

Ms. Vasu: Yes, we do the device certification whether it is an Apple device or an Android device. The device certification process will occur in both cases. The difference is the location of the token. One is in the secure element, while the other is in the cloud and in the device memory. Basically, to compensate for the lack of a secure element in the cloud, we have the limited-use key that I explained earlier. But as far as device certification is concerned, we certify in both cases.

Mr. J. Williams: One of the interesting things about trying to protect all these different systems is that you have to look at the business case. What has happened in the U.K. over the last three or four years is because of the movement of transactions to card not present, for reasons as we have heard earlier of the adoption of EMV, a lot of merchants wanted tokenization services. What has happened is the acquirer or the payment service provider sitting between the acquirer and the merchant has offered these services to the merchants to solve that particular problem. Of course, the business case for the merchant is it saves their PCI scope, minimizes their costs. But the business case for the acquirer is that it makes the merchants that much stickier as clients. So why have we not seen this as a business case so far? Is it just that we have not seen as much card-not-present fraud in the United States so far?

Mr. B. Williams: From our perspective, we do not create that sticky relationship. So in our contracts, they are allowed to convert back. We also have an instance now where you do not have to be connected to First Data processing to use this solution anymore. But I think that probably has hindered some of the adoption because one of the big problems is that merchants are afraid of technology lock-in. I think we are all afraid of that. We are all afraid at some level that we do not want to get stuck into some technology that ends up hurting us long term. So that may have hindered things for now.

Mr. Schmalz: I have seen white papers floated and proposals to have—I do not know if I am using the right term—but sort of a tokenization service proxy where you go to one spot and it would ping the various tokenization service providers. It would do translation. So if you had a First Data token, you could send it, it would talk to First Data on your behalf and get the PAN back and then maybe create another token for another acquirer it is using. I think an association for hotel owners might have come up with that proposal, which would solve that problem. Right now, the tokenization solutions seem to be acquirer specific; of course, the reason is because it is a good business case for them to do it. You need to find a business case for either cooperation or for some third party to take over that still allows the acquirers to play a part and add to the security.

Mr. Spittler: We are talking about tokenization. In what sense is tokenization important to competition? I have seen that we are more or less going to concentrating all the tokenization service to networks, instead to having usage of tokenization by all actors like acquirers, merchants. In which sense is competition increased when you use tokenization?

Ms. Vasu: I am just going to rephrase your question to make sure I got it right. So the question is we have a network tokenization solution, and who is the competition for that?

Mr. Spittler: My question is, is it competition? How do we increase competition with tokenization? Because I have the impression that it is more concentrating on networks instead of all actors.

Ms. Vasu: In the current set of implementations, we have the networks who are playing the token service provider role, but in the EMVCo specifications, we are not restricting it to just the networks. A large issuer, a merchant or processor could play that role. We do not have requirements today, and that is what the next version of the specification is working toward in terms of other entities becoming token service providers. Now, in the case of the network, it was convenient because we see both sides of the transaction from the merchant acquiring side, and the issuer side, and we have the numerics and the BIN management in place. But we are not restricting anybody from becoming a token service provider down the road.

Ms. Crowe: And I think that is our last question. Thank you.

Mr. Dubbert: Thank you, Marianne, for coordinating the panel, and all the panelists for being with us today. I will be sure not to throw the term “token” around too much; making sure I understand what that means.