General Discussion

Managing the Threats to Data Security

Mr. Santhana: This question is for Vernon Marshall and Liz Garner. The future of fraud, as you all discussed, is in card not present and online account takeover. But if you look at the problem, we can do simple things that we are not doing today. On the merchant side, there is no standardization on capturing device data, IP data and proxy piercing. On the network side, they are unable to take device data and IP data and pass it to the issuers. So any thoughts on how we can improve those and capture all this data? You talked about machine learning. Machine learning can use that IP data and device data to do a wonderful job of looking at the devices that are related to a household, related at the account level and identify across different merchants as to what devices are using which card. So any thoughts on improving the data capture part?

Mr. Marshall: Ultimately 3D Secure is going to have to cover some form of device ID, and the problem is the large number of different device ID schemes. So it would be helpful if one of those becomes dominant, and it needs to pass IP address. I agree that is significantly helpful. 3D Secure needs to provide more data. It cannot just be reliance on a fixed password or a dynamic password because that too easily can be compromised in this environment.

Ms. Garner: You said in your question, standardization, no standardization. Standardization is a difficult word to use when we are talking about security because there are challenges that go with overstandardizing something. So back to my main point, it is important to lay the groundwork in an open competitive environment for how these technologies are going to work. We should not leave the development of specifications up to EMVCo and PCI when you have only a certain amount of input from different stakeholders at the table. No voting rights by merchants or really anybody outside of American Express at the table here. That is the first step. It is a slow, painful process sometimes to go through an accredited standards-making process, but we have not changed the technology since 1972. We are on the verge of changing the technology to go into the digital environment. We have to get it right.

Mr. Horwedel: My question is this, in view of the fact that neither the merchants nor the merchant processors have any voting rights in any of the networks, in PCI, in EMVCo, and in view of the fact that the basic card product has remained unchanged since its inception 40-some plus years ago, why is it the merchants' and the processors' responsibility to protect the networks and the banks from their own product?

Mr. Marshall: I would get back to Tyler Moore's presentation this morning. For EMV to be implemented, the industry needed incentives for everybody to issue EMV cards and merchants to issue or build the EMV capabilities. Otherwise, EMV would not happen. So liability shift was the only way EMV was going to happen.

Mr. Carr: And we believe in encryption, point-to-point and end-to-end encryption, and I am not sure what more we can do than that.

Mr. Taylor: This is not for Liz because I know what her answer is going to be. I am going to make a statement, and I would like to get a comment on it. Increasingly, we talk about protecting the system and the ecosystem, and all the billions of dollars we have thrown at it, and you look at the card brands' own fraud numbers. We have not materially moved the needle which says the other guys are out-innovating us when it comes to protecting the system. Is it time for us to start forgetting about protecting the system, and start figuring out and focusing on doing clean transactions in dirty systems? And a second follow-on question, is EMV not really a deterrent and a distraction from doing that? Would we get better bang from our buck in trying to, to Bob Carr's point, take the value out of the transaction and the data out of these billions of endpoints that we cannot manage, instead of trying to lock down those endpoints because we cannot manage them?

Mr. Marshall: You need to solve the problem in both places, so both protecting the data in the first place, which we will be discussing this afternoon, but also protecting usage. EMV makes a huge difference in reducing the value of stripe cards. There is so much theft of stripe information at the moment because it is so valuable and it will be much less valuable after

October this year. So you have to do both. Probably though the quickest thing to do is to protect the usage.

Mr. Carr: I just come back to Governor Powell's comment. He said, "Preventive measures are not adequate." I completely agree. There is a lot of embezzlement in this world, and where does it come from? It comes from the trusted employees in companies. So we trust that our employees are going to all follow all the PCI procedures properly. But they are human beings. Sometimes they are careless, sometimes they are incompetent, sometimes there is a financial incentive for them to cause problems. All the preventive measures in the world are not going to prevent that problem with your employees. That is why I do not see why we do not spend a lot of energy, it does not cost that much, to do the encryption. It is a couple of dollars per device. And yes, you have to upgrade the devices, but it is not that expensive relative to going to EMV. But the industry has determined that encryption is not a significant part of the solution. I do not understand it. We have no skin in the game, by the way. We do not have any proprietary interest in anybody's encryption system. It is just, why are we not encrypting this stuff?

Ms. Walker: We have heard a lot about the private sector pieces on instant solutions, but I am curious. We are here at the Fed. What is the Fed's role in this, or what are you looking for from the Fed on this?

Mr. Marshall: One thing I would love to see happen in the United States is the same type of reporting that we have in France and the U.K. It would be very useful to be reporting fraud loss at a fairly granular level. It would be useful for us as a card issuer, useful for merchants and the networks. That is the most obvious thing the Fed could help with.

Ms. Kitten: I will jump in here too. There was discussion three years ago about whether the Fed would step in to oversee this migration to EMV, and it was made clear that the Fed did not want to play a hands-on role there. So it has to fall to the private sector.

Ms. Garner: The role the Fed is playing now is a good one in bringing stakeholders together to talk through a lot of the issues. That is a real positive. We are excited about the potential that the Secure Payments Task Force has. Publishing papers like the one they published this morning is also great. We do need to do more from a data collection standpoint. That has been a theme throughout, and is something we would love to see too. From the merchant perspective, there is very little data available to us as well. That is one of the challenges when people look at, do I need to be going to EMV right away. Well, show us some more data that shows we need to get there yesterday instead of tomorrow.

But the bigger thing here is when we are talking about the policy dynamics, and this is one reason I liked how Adam Levitin laid it out, the public versus private trade-offs. In Washington, a lot of the regulators are looking at how do we respond to breaches? Do we pass a breach notification law? Do we share information after we are dealing with a breach, sometimes before? There is a lot more we can do in the fraud prevention space, and I am going to say something kind of out there that may be unpopular here at the Fed. But the Fed has a role to play here already. They have the regulatory authority to intercede in the marketplace. There is fraud prevention adjustment language in Reg II, also known as the Durbin Amendment, that allows the Federal Reserve to prescribe standards whereby issuers can receive an interchange fee/fraud prevention adjustment, and it asks them to take into account things like transaction mechanisms. Is it a PIN transaction, is it a signature transaction? You know the data that we put up on our slides about fraud losses, card-not-present fraud being borne 70 percent by merchants. Where is the trade-off here? We talked about if parties do not have the incentive to protect the data, do we get to where we need to be? And right now, issuers are not bearing a large portion of card-not-present fraud, and it is one of the fastest growing types of transactions in the United States. And one of the other components of that legislative language says the Fed should consider, what are the resources expended by all parties to deploy these technologies, and EMV case in point, some of the third-party groups out there said, you know, this is an $8 billion project for merchants, and less than $2 billion on the issuing side. I do not know if those are right, but if we start to think about, what are those trade-offs, there is a potential role for the Fed and we would love to see them get more involved under their current statutory authority in that space.

Mr. Carr: I just want to jump in and say the Fed is arguably the most respected institution in the ecosystem, and a lot of startups are innovating and trying to create solutions, some of the established players as well, and it would be great to have best practices recommended by an authoritative organization. That would be a lot better than what we have now. Look at what we have now. We have vested parties interested in promoting their own solutions. I do not think it is working very well. And Eric (Grover), with all due respect, I do not think the free market system is at work here, before you ask.

Mr. Marshall: That said, it is worth remembering that the United States has the lowest fraud losses as an industry compared to other countries. We have a lower fraud loss than France, for example, as an industry. We have to have some sense of optimism that the free market system here is working at producing solutions. I am not saying we do not have challenges, and we were late implementing EMV. One of the reasons we were late is that our fraud control process has worked pretty well, even with ridiculously old magnetic stripe technology.

Mr. Horwedel: Is that because we have the best telecommunications in the world?

Mr. Marshall: Yes, that is definitely true. Certainly, over the last 20 years, we have benefited from being able to authorize 100 percent of transactions where it has taken much longer in other countries. That is true.

Mr. Santhana: We are banking a lot on EMV right now, but as Governor Powell said this morning, if you look at that fraud incident that happened in 2013 where $40 million was compromised in 24 hours in 26 countries, cybercriminals actually went into the authorization system of the prepaid card issuer, and changed the limits. On the EMV side we are deploying, the dynamic card verification value (CVV) verification takes place at the exact same location, at the authorization system. Disabling that rule could allow counterfeit cards to transact because you are not checking whether it is an EMV card coming through. Do you foresee something like that? Are you fearful of that?

Mr. Marshall: I suppose it is possible. I think it is highly unlikely given the amount we have invested in cybersecurity, and that would be true of all of the major issuers.

Mr. Moore: I want to ask a question on a slightly different topic, going back to Vernon's points about machine learning and its value. There is a conversation about trying to get extra information to help make better decisions, and talking about getting device ID, IP address, I can see it evolving toward getting behavioral patterns of users and looking for deviations from their online behaviors. And the more we go down that road, the more likely we get into issues concerning privacy. I am wondering about your thoughts on that, whether or not as we start collecting more data, passing it back to different players in the system, about the behavioral profiles of cardholders. Could that lead to an enhanced privacy risk by collecting and disseminating that data?

Mr. Marshall: Yes, that is a good point. The data has to be protected, only used for the purposes of fraud, not for any other purposes, and it has to be made secure, and for limited purpose. And the amount we collect should be limited entirely to what we need to control the transaction. I do think it is reasonable to receive an IP address and device ID for somebody that is making a transaction at a retailer. And retailers, of course, use that information to date to do their own fraud prevention. So it is reasonable to expect that the card issuers also, if they receive that data, could use that information to further protect the transaction. But I do agree there needs to be a ring fence around the use of that data.

Ms. Garner: I agree with that, and one of the things that scares me about EMVCo is they are trying to solve a problem we raised with the tokenization solution that they have out for comment right now. They have a payment account reference (PAR) number, but it seems like a lot of information could potentially be coupled with this PAR, where there is more insight into some of the transaction data, as well as other items we could couple with that data like a rewards program, than I am comfortable with as a merchant. The last thing any of my merchants wants is somebody to be able to come in and sell their competitor's purchasing data. So I agree, and it comes back to, for me at least, moving this more into an open standards environment to ensure we are not allowing people to gain market share by competing in that proprietary standards environment like the paper you guys put out says.

Mr. M. Williams: As a merchant, I agree with several of the comments that have been made about the use of PIN. It baffles me that we are going to all this effort in the industry and we are not taking the opportunity to fully implement chip and PIN. But what is more frustrating is the way it has been messaged, part of that being a comment I heard earlier, I am not sure who made it, "chip gets us halfway there," and then Vernon, you made the comment that this takes out 60 percent of counterfeit. I will politely and respectfully disagree with your comment that card not present is not linked. There are plenty of Fed studies that would indicate they actually are linked, and in some of those studies I have seen, at least two of four countries that were studied actually saw an increase in fraud following the implementation. Now that is total fraud, but I get the sense that we are communicating this, especially to consumers and others that are not in this room, that this is a solution to the problem. I am curious, Vernon, for your response. What happens when there is a breach following the implementation of EMV, and those cards are able to be used online? How do you go back to consumers that you have currently told this is a solution, this will protect you, and then they are just as exposed? That is question one. How do you respond? And question two is, I am curious to hear from your perspective, what is American Express' justification for not putting PINs on cards? The only thing I have heard thus far is that it just is not what the industry is doing. But I assume, given that American Express has PIN cards in other countries, that there is some rational explanation for why it is not a good idea in the United States.

Mr. Marshall: I will start with the second question. At American Express, we have made all of our cards PIN-capable, and we are certifying merchants to process PIN. We will be ready to roll out PIN if the industry makes that move. What I want to avoid, and what American Express wants to avoid, is having to enter your PIN in one of every 20 merchants; that would be a disaster because you are going to forget your PIN. So the PIN rollout needs to be something that is orderly, and it needs to be when there is a significant base of merchants that are already accepting PIN, and we can roll this out at one time. I also think it needs to be an industry standard. Otherwise, it is going to be confusing to consumers to sometimes have PIN on some products and not on others. So we have made the decision to be ready for PIN and we have invested in PIN, but we are not yet ready to deploy it. But we expect it is likely that we will be implementing PIN at some point.

On the issue of compromising, if you think about it, for card-not-present fraud, you need a lot more information than just the 15-digit or 16-digit account number. All the compromising that leads to card-not-present fraud, you need the name, you need the address, you usually need the email address, you need the phone number. So for card-not-present fraud, the compromises for that are not point-of-sale malware, literally you have to go to the source of that data which is usually an online retailer to start with. So you do not see fraud, the Target situation, and any of those cards that were compromised at the point of sale, those details were not used to commit card-not-present fraud because it just does not have all the information criminals need to make the transaction take place.

Ms. Garner: I would have to respectfully disagree and I will just tell my own personal consumer story. I was traveling in Brazil last summer. I am a bit of a soccer fan. And I dipped my chip card at a card reader, and I could see when it prompted me for PIN, and I did not have a PIN, they were handing it over, "Hey, enter your PIN." The tour operator looked at me like, "Oh, you do not have a PIN on this card?" I was like, "Oh great, this card is done." It was done. Within 24 hours. They knew nothing about me other than the name on the card and the primary account number. Maybe they pulled the expiration date while I was not looking, but they did not have my email address or anything else, and they were making charges back to U.S.-based websites before I had left the city that I was in in Brazil.

Mr. Marshall: Without the details, OK.

Ms. Garner: Without all those other details.

Mr. Marshall: I guess it is possible. Most merchants would normally be checking the Automatic Address Verification (AAV), Address Verification Service (AVS) in the Visa/MasterCard world, they would be checking name and address for every transaction, and they also would be checking the three digits on the back of the card.

Ms. Garner: I am not going to throw anyone under the bus because one of them is one of my members. There were two very large sophisticated merchants where fraud was perpetrated online.

Mr. Marshall: You could advise them to at least do the minimum checking; that would be kind of helpful.

Ms. Garner: Well, we joke about this. But then people push back on me all the time and say, "Well, PIN is a static data element." Well, Card Verification Value (CVV) is too, and we talk about a CVV capture as an extra authentication tool online. How good is that really? It is on the card. So somebody could have easily copied it off my card. Maybe they did it that way.

Mr. Marshall: It has gaps, but it is terrible to not check it. It makes fraud very easy to commit if you do not check it.

Ms. Garner: I promise I will not give you a hard time, so we will stop there.

Mr. Santhana: I have a question on network tokenization. I like network tokenization because it takes card numbers out of the ecosystem completely. I do not understand why merchants need to have a card number to do a transaction. However, we have heard complaints from merchants saying they cannot track their loyalty programs. So what is it going to take to wean the merchant community away from card numbers as we move progressively toward network tokens?

Ms. Garner: I think there are two other reasons why merchants want access to the primary account number (PAN) and one is our own transactions fraud monitoring. We have not had very good e-commerce solutions in the past. So tokenization is not new by any means. There are several e-commerce merchants who have deployed some sort of a tokenization-like security technology for years. I was at an event with Amazon last fall where they said this is definitely not new to us. So transaction fraud monitoring is one area where we use that PAN and rely on that PAN to know the customer. And then customer exchanges and returns—that is one of the biggest challenges with the EMVCo token solution that is the back end for ApplePay. I cannot share an account with somebody necessarily and go back in with my Apple device and make a return or any type of exchange at the retailer because you cannot consolidate those accounts. There are some big challenges with how certain tokenization solutions are being deployed. That is not to say all tokenization solutions are created equal; I am just giving one use case.

Mr. Moore: I have a question for Mark Carney because he has not been loved very much in this panel on the Q&A. One thing I raised, and it came up here, is that there is huge variability in QSA quality, and the general evaluation quality for compliance inspections. I made this argument that it is due to information asymmetries, and maybe some adverse selection going on and the merchant is not selecting the best evaluators. I wonder what you or anyone else might think about how we might improve this process so the outside evaluations and certifications that take place are more valuable and actually say something about the security you are trying to evaluate?

Mr. Carney: I love that question, and I love having a question, so thank you. The initial Qualified Incident Response Assessor (QIRA) list was six firms. FishNet Security was the seventh. It was a very, very tightly controlled assessor list, basically for post-data breaches. I thought the quality of assessor sought by those that controlled this list was critical. They demanded a lot of qualifications, and the process to become QIRA certified took four to six months. Visa upheld a very, very high entry point for a consulting firm to come in and represent Visa, MasterCard, etc., in these post-data breaches. To me, that is the best example of the PCI certifications that are out there. Certifications for Approved Scanning Vendors (ASV), Payment Application Data Security Standard (PA-DSS), the QSAs, and others are much different. When the PCI council took over the QIRA program, now called the Qualified Forensic Investigator (QFI), unfortunately what was observed was a watered-down skill set. At that time, the barrier for entry was lowered, and the quality of consultants representing QFI firms suffered. Not only that, the pricing pressure came along with new and more QFI firms making the list. Forensic investigators are not cheap to hire and require extensive training, so you have to have a bill rate that is correlated to the cost of a skilled person. Once that skill set gets watered down or there are more firms on the QFI list, then those are natural things that can hurt the quality of work for post-breach investigations provided to merchants/service providers.

Mr. Dubbert: All I can say is I am amazed at how much ground this panel covered in an hour and 15 minutes. That is a tribute to each of the panelists. Tracy, thank you so much for your coordination.