# General Discussion

## *Role of Industry Collaboration in Payments System Security*

***Mr. J. Williams:*** Now I would like to open the questions to the audience.

***Mr. Schmalz:*** One comment and a quick question for Liz Votaw. The comment is that the use of the certificate-based authentication mechanisms means you do not have to protect secrets on the server side. Did you mean that in the context of the biometric templates, or in the context of symmetric authentication mechanisms, which require secrets on both sides?

***Ms. Votaw:*** I meant it in both cases. There are no biometric templates stored on the server side, it is an asymmetric key environment, and it is a public key that is stored on the server.

***Mr. Schmalz:*** But the server has to have a public-private key paired to authenticate itself to the endpoint, so there is a secret protecting its private key. If that is compromised, you can do a man-in-the-middle attack, so it is equivalent to compromising secrets for a symmetric key system.

***Ms. Votaw:*** There are going to be some vulnerabilities, yes, but it is certainly better than where we are today with passwords.

***Mr. Schmalz:*** We do both, and you have to balance the advantages and disadvantages.

***Ms. Votaw:*** Sure, and RSA is on the board of the Fast IDentity Online (FIDO) Alliance.

***Mr. Schmalz:*** Yes. The other question is something that has been an issue with public key systems since their inception. There are a couple of issues. There is registration or provisioning of the certificates down to the endpoints, making sure that the owners really are who you think they are from the server side, and then there is the revocation question. So everybody is familiar with SSL (secure sockets layer), where the revocation issue really has not been addressed, and many times there are issues with just client's auto authentication. Are you addressing the registration and the revocation questions?

***Ms. Votaw:*** When you look at FIDO, the registration is trying to solve for the password problem, but this is a step in the right direction. It is not going to happen overnight. Everything is tied to whatever the trusted session is for the party that is employing it. When you go to register, you are only as sure that it is the person as you were before you implemented FIDO. You have to register it to your existing password structure. You have to be able to know. If you look at the registration process, you would go into a trusted session and then register for FIDO with your device. Everything is only as strong as the password, as long as we have passwords. They are still the start of that process. But when you look at things like what Microsoft is doing, where you are going to be able to create an identity on your Microsoft Windows 10 device, and then their passport would allow you to transport that as an identity into a line of business, you are starting to get to a passwordless environment.

***Mr. Hamilton:*** Thank you very much. That was real interesting to get the different perspectives on collaboration and I am a true believer in industry collaboration. It is critical for success. One thing I worry about in trying to encourage industry collaboration in Australia is the problem of overlapping initiatives. There are many well-intentioned, well-thought-out attempts to solve industry problems which run across each other because you need to get the same group around the table over and over again to solve a slightly different problem. MasterCard, for example, is on all four of the groups we just talked about. This is understandable, it happens all the time. I am interested in the perspectives of the panel on how you manage that problem, that you can have so many different well-intentioned, great ideas that struggle for success because there are so many of them?

***Mr. J. Williams:*** That is a great question Chris. I was at an EU cybersecurity workshop about two weeks ago and one of the challenges they had was trying to categorize what we mean by cybercrime, because if you talk about it as online security, or as e-fraud or e-commerce fraud, or potentially even theft where it is done by an electronic mechanism, or cyber-enabled fraud or theft, then it gets sent down a particular route within law enforcement. There are particular task teams looking at each topic. The result was that if you called it cybersecurity it was everyone's problem. So how do you solve this problem?

***Mr. Bretz:*** A couple of observations: The groups that execute will probably survive, and that execution, much of it is built on the people in the groups and on trust. You have different companies, different technologies involved. So the question is do they trust each other, can they work together, can they execute? People ask us why the Financial Services Information Sharing and Analysis Center (FS-ISAC) is so successful. It has taken us 14 years to build trust and the network of information sharing. Much of that is group dynamics and can you execute. The groups that execute probably will survive on the standards side. That is leadership; it is the passion of the people in the group that makes a difference. I do not think there is one answer.

***Mr. J. Williams:*** Nancy, since MasterCard is one of your members in the Payments Security Task Force, do you have a perspective on overlapping the other collaboration efforts?

***Ms. O'Malley:*** Yes, and I thank you for pointing out that we do support all these efforts. We spend a great deal of time ensuring that we understand the mission of the particular group and that it remains focused on that mission. When we formed the Payments Security Task Force, one of the first things the PSTF said was, as a collective steering group, we want to make sure we supplement the work that is being done, for example, by the EMV Migration Forum. We do not want to interfere with that, and maybe we tackle problems that particular forum has not been successful in tackling and add value in what we bring to the overall equation. Our goal was not necessarily to be the organization that survived beyond this particular market event. Our goal was to bring the power of those particular organizations, which represented 80 percent of the market on the issuing side, to bear, to advance the work of other organizations. It was supportive at the outset in what it hoped to accomplish. Now it has evolved further because bringing safety and security to the marketplace is not just about EMV. It is about other technologies that need to be brought to bear. As we bring EMV to the market, we also are working to advance adoption of these other technologies so that years hence we will really have what we can at least perceive today to be the most secure marketplace that we can build. That is entirely about collaboration because we cannot do it alone. We have to listen to and respect all the opinions of all of the players in the market, and the impacts of any particular decision that might be made in one technology will have on their businesses. We have to do a much better job of bringing those constituencies together and working together. Sandy commented on some of that, and we absolutely embrace the importance of doing so.

***Ms. Kennedy:*** Fear helped drive our collaboration. There had been significant finger pointing after the Target breach, and we felt that to attack this in a way that would be meaningful to Capitol Hill and the statehouses, we needed to do it together and collaboratively. Any time we can come together and find solutions as a payment ecosystem, it is always going to be better than when Congress tries to find those solutions. It was really almost a fear factor that drove the participation and the commitment and the results.

***Mr. Horwedel:*** In keeping with what you were suggesting about bringing together these groups, is there a further opportunity in making this more of an international flavor? We are doing things in the United States that are counterproductive, like chip and choice. It creates seams between the markets; problems for consumers. It is ridiculous that we are doing that. Should we not have, for example, more of an international effort to get rid of these seams in our payments system and deal with security matters on an international basis so that fraud does not simply migrate to the United States?

***Mr. J. Williams:*** A great question, one I certainly remember having discussions about with law enforcement agents who were saying if we were really successful in the U.K., we move all our fraud to France. I would not agree with that. I think that is the wrong thing to do. Nancy?

***Ms. O'Malley:*** Taking an international approach is absolutely the right thing to do. There is no question about it that MasterCard, being a global company, brings that. We believe we bring that flavor increasingly to these conversations. And we are cognizant of our responsibility to do that. Certainly, others who participate in some of these forums with us, like our competitors, are global companies as well. In the context in which we operate as a payments ecosystem, we recently have been focused domestically, but there is a unique role that we should play in the global marketplace. We have the most significant emerging technology companies located in the United States. We have major payments networks. We have some of the largest banks in the world, and we have a very diverse and technology-accepting environment. All of which should contribute not only to our responsibility to advance the adoption of technologies, but also ultimately to lead the way. We have obstacles in our way, but I am excited about some of the things we are doing collectively and collaboratively to overcome those obstacles. We are working more together than we have in the past. It is not perfect. There is a lot more work to do, but I think some of the work the Fed is doing is also going to be a key in allowing us to advance as leaders in the marketplace, which is a place the United States should be.

***Mr. J. Williams:*** I agree. I think that is what we are seeing. Charles?

***Mr. Bretz:*** I used to work for an international bank, and I had the pleasure of working with colleagues from about 15 countries. I realized that there are legacy payments systems in each of those countries, and legacy technology systems, in other words, telephone systems, the Internet. An international system is a good goal, but I do not think you can completely do away with all those legacy systems, whether it is a payment system of the United States or in another country. It takes a while for those things to coalesce. It is a worthy goal, but the more you try to get an international standard, the more you have some difficulties. Also, you have currency issues and capital controls in countries. Those types of things are complex.

***Mr. Carlson:*** Looking to the future, say three years from now, after EMV has been implemented and some of the task force work has been done, what do you think is going to be the major focus of private sector collaboration? And there is an additional question to that. Are we organized sufficiently to address those issues?

***Mr. J. Williams:*** Liz, can I direct that to you first? When we all have FIDO-enabled devices.

***Ms. Votaw:*** We talk a lot about does FIDO exist in three years, or does it become so much a part of the ecosystem that it does not need to exist? From a FIDO perspective, whatever the technology is today it will have evolved in ways we cannot imagine three years from now. The pace is so crazy, and you need to have your eye on the ball about keeping the standards and keeping the principles. I think we will still be around in three years focusing on the same issue.

***Mr. J. Williams:*** Sandy, what does your future look like?

***Ms. Kennedy:*** Our partnership has concluded, but if the need arises, we certainly would be comfortable reaching out to the Financial Services Roundtable and the financial services industry again to look for those areas of collaboration, especially as we work to provide a seamless environment for our customer, whether it is mobile, digital, or in-store. That is our key asset, our customer. If there are opportunities for us to remove challenges, work on challenges together, I certainly think we would move forward on that.

***Ms. O'Malley:*** The Payments Security Task Force, like the Cybersecurity Partnership, was not designed to have an indefinite life. However, there is a real interest in continuing to tackle some of the new and emerging issues—the need for information, for education at the CEO level, in the board room and the cybersecurity space. As long as our membership continues to ask us to reconvene and tackle critical marketplace issues, we perceive that as the need that should be addressed and most likely we would continue to do so. These things will have a life because as technology advances, and unfortunately as fraudsters innovate, we will see an ongoing need to adapt and adopt and to accelerate our efforts. Speed is a big issue for our marketplace, and we have to find ways to move forward faster to move with the pace of our competition, the folks who want to commit crimes against us.

***Mr. Bretz:*** It will be amazing how technology develops over the next two or three years. We do not know what the next cool payment technology is going to be, and somebody is working on that right now, or teams are working at that. It is going to come out, and then we will be reacting to that. How do we secure it? How do we put it on whatever device we are carrying? And on the criminal side, the same thing. They are very well-funded. They are making a lot of money right now. So we will be reacting to their innovation.

***Mr. J. Williams:*** Hopefully we can turn off the tap of cash funding them, and then maybe they will go and do something else, or maybe not. Any questions from the audience? I have one that extends the last question. Assuming we are really, really successful, and we completely secure the card payments system, where are the fraudsters going to go next? Liz?

***Ms. Votaw:*** That is like the stock market. If we knew that, we would all be much better off. I do not know. Where are they going to go? They are going to go wherever the weaknesses are. Wherever we are not is where they are going to go.

***Mr. Bretz:*** A member I cannot identify said yesterday that their fraud on the RDFI (receiving depository financial institution) side for the ACH (automated clearinghouse) was up double this year. They shared that with some other members, saying, "Gosh, I do not know if our numbers are that big, but we are seeing an increase." And then we are seeing faster ACH payments coming to the United States and that it is going to create opportunities to reduce risk because we will know faster about that transaction—is it a good transaction or bad transaction. But we also are having a problem in the United States now with business email compromise, where wire transfers are being originated fraudulently. Fraudsters are tricking the business into sending a fraudulent wire. In the United States, most of those are going to Hong Kong and China, to Russian-speaking cybercriminals. But they are sending it through China. And you were saying in the U.K. what they are doing with faster ACH, they would send it to a U.K. bank and then they would use the faster payments, which would be like a fast ACH, to send them to multiple endpoints. If we have that same thing in the United States, we are going to have to build risk technologies to try to mitigate that.

***Mr. J. Williams:*** Absolutely. There are necessary tools we do not currently have in our arsenal. In the U.K., we have seen an increase in fraud against direct debits. Account details of individual customers being provided to ordinary businesses, who then collect money. It is not for the individual, it is for the fraudster, and they are buying some goods or service. Unfortunately, it is on the rise. Typically, it takes about six months for a consumer to notice they have fraudulent transactions on their account.

***Ms. O'Malley:*** Some things, certainly card not present will be the most immediate attack. The work that Liz and FIDO are doing is probably one of the most critical things we could be investing in right now, because we believe and have seen that one of the next waves of migration would be some sort of account takeover activity. Our concern is that although there have been attacks on databases where we have critical PII (personally identifiable information) data, they are spreading those attacks. And the purpose of obtaining personal information is for the takeover of an account. Some recent data breaches are in nontraditional spaces that we do not usually think about from a payments security perspective as being impactful on our business, but they absolutely can and will be. So how do we link those together? How do we understand who those criminal groups are? How do we understand the target, what they intend to do with that data, and then how do we inform our financial institutions to protect themselves? All of that is important work that the FS-ISAC does. Then there is the work that Liz and her team are doing to build solutions to provide better authentication methodologies for our financial institutions so they not only can authenticate at the time of either provisioning a mobile device or opening an account, but also at the point of transaction. Those are important bodies of work that will contribute to solving what is likely to be the next wave of attack.

***Mr. Bretz:*** I have a comment about card-not-present fraud. When EMV was implemented in Europe, some of the fraud shifted from card present, because counterfeit cards are difficult to create after EMV, to card not present. But Nancy's task force has recommended that you put in an EMV terminal. They are also stressing point-to-point encryption and tokenization. The combination of those three might protect the PAN (primary account number) even if there was malware on the system. The PAN might be encrypted or tokenized, so it would not be of value to the criminal, so they could not do card-not-present fraud. It will be interesting to see what happens in the United States with the combination of those technologies. Also, you mentioned surveys that you have done. It would be interesting to see how fast those payments systems are implemented, and I say a more secure system that would have EMV, point-to-point encryption and tokenization. And I know you are trying to track that. Some of the members I support are also trying to track that. It will be interesting to see over the next couple of years how fast that technology comes in.

***Mr. J. Williams:*** So, Sandy, if we can solve your card problem, do you think the fraudsters will start trying to redirect your supplier payments?

***Ms. Kennedy:*** We do not believe chip is the only solution. It is an interim step, but it is important that we are constantly evolving, looking for where the fraudsters are going and protecting our customers. They expect us to collaborate, work together and find those issues that can make them safer in the end. Who knows how we are going to be shopping in five years, with our Apple watch or our mobile devices, or who knows? But it is important that we stay steady and consistent in our drive for making sure the payments system is safe no matter how our customers choose to shop.

***Mr. J. Williams:*** Before we wrap up, I would like to ask each panelist to leave us with a closing thought to take to our organizations and try to implement. Liz?

***Ms. Votaw:*** Other than joining the FIDO Alliance, consumer behavior is what is going to drive pretty much everything. As companies start trying to solve for the security piece, we have to be thinking about the usability and consumer side in trying to find that balance between usability and security.

Do not assume consumers are going to change their behavior, because the model has not really changed for them. It only has changed for us. Keeping the consumer king will keep us all on the right path.

***Mr. J. Williams:*** Consumer friction and consumer behavior. Sandy?

***Ms. Kennedy:*** We have a shared enemy and a shared customer. The more we collaborate, the more we work together, the more we can trust each other on these big issues, the more successful we are going to be in protecting our customers.

***Ms. O'Malley:*** I could not agree more. Some of these initiatives have clearly demonstrated the power of collaboration, and what we can do when we come together and agree on and move forward with agendas that advance safety and security. There is a global role for us as a marketplace that is equally important and we have to be mindful and respectful of that. We can achieve a great deal in a very short time if we put our minds to it.

***Mr. Bretz:*** A little different thought. If and when you are attacked, do not feel alone. Rely on your colleagues within FS-ISAC, or other partner organizations, to help you with that. Share information about the attack and ask them for help. We have seen dramatic results when those attacks happen and people have asked for help and had a rapid response. That is my closing thought for the day.

***Mr. J. Williams:*** Thank you. I will leave you with one thought of my own. When I was preparing for this panel, I was dictating notes into my iPhone, and as it got the information, it misread data "breaches" as data "britches." I think that is a topic for a completely different conference. However, with the "Internet of Things," and wearables becoming more and more important, who knows what will happen in 10 years? We will be talking about data breaches within your britches. Thank you.