Role of Industry Collaboration in Payments System Security

Moderator: Jonathan Williams

Mr. J. Williams: We are looking at the industry role in collaboration and how we can help protect our financial institutions and the payments systems from all the attackers that we know are out there. I would like to thank the Federal Reserve Bank of Kansas City for giving me such a wonderful panel of eminent experts in the field, each representing a number of different collaboration efforts, and they will be talking about that later. To avoid any doubt, they are representing their collaborations and not the organizations you might otherwise associate them with. They will be talking about how they work together.

I am going to set the scene for what is the role of collaboration. Some key questions we need to ask ourselves are those I am sure you got in third or fourth grade when you were trying to tell a story. They are the questions about who, what, when, how, and most importantly, why. And the reason why we are looking at collaboration is obvious. We cannot individually solve the problems, protect all our organizations, have all the intelligence in any one business. Therefore, we need to work together, share intelligence and develop common standards and common systems. We need to work for the societal good because all these things are trying to protect the whole system, not just our individual institutions, but a whole set of payments systems to protect all of our customers. That is the real driver. We need to act from a moral point of view to restrict the bad actors from gaining overall control of our payments systems. No one has all the cards, and we need to try and understand what key points we need to bring together as part of these collaboration initiatives, and to work together to be able to properly attack them.

There are different types of collaboration, and when we were discussing this in the run-up to the conference, there were a number of different ways we categorize collaboration. We can certainly categorize it in terms of who

are the actors that are collaborating. Is it purely the financial institutions? Is it IT vendors? Is it service providers? Who actually needs to work together to provide all of the expertise to combat the threats that we see?

There is a question of what we collaborate on. Is it purely on the systems security side, or do we need to understand how that might impact our business processes? Do we need to set standards within our business of how we deal with clients and how we deal with other actors in the system? And there is certainly a question of how we deal with external parties, including our consumer customers whose view of security tends to be fairly lackluster.

There is a question of when we engage. Are we setting standards so that we are protecting our businesses, or is it a post-event collaboration to try and ensure we remedy the fact as quickly as possible? And then there are many different ways we can actually engage. Certainly by looking at information sharing, but also by working out whether there are common means of procuring services. Maybe there is a common service we need to develop to protect our organizations. There are a number of different ways we can work together, and as I pass to the rest of my panel, they will be tackling these particular discussions for each of their different collaboration initiatives.

I would like to finish by giving you a perspective on some lessons we can learn from history. In the interest of transparency, I am not paid by any of the European tourist boards whose castles are mentioned here, and these are not potential scenes or sets for "Game of Thrones" either. However, I think there are a lot of lessons from the Middle Ages that we can learn from. We talked about ensuring our businesses are secure. Yesterday, we were talking about building the walls higher, and these are great examples of high walls. But there are all sorts of other protection we need to think about. Walls are one sort of protection. However, if you built a castle which only had walls and did not have any gates to get in or out, that would be pretty useless. Therefore, we need to think about the security of who we let into the castle, who we allow to do business, and how we identify them, who we let the drawbridge down for, who we close the portcullises on. The castle at Chinon in France (upper right, facing page) is a great example of the purpose of protection. That castle is geared to protect a particular physical feature, it is that particular mount. Therefore, one of the key things we need to think about when we are designing our security is to design it around the business, to make sure it fits the business need. It would be perfectly possible to

Cybersecurity Lessons from the Middle Ages

create a wonderful castle, maybe something like the Disney castle, which did not fit a business need and was not protective of all of the assets and all the data inside. Therefore, I think we need to be very focused on exactly what we are trying to protect.

Now I will hand the program across to Charles Bretz from the Financial Services Information Sharing and Analysis Center (FS-ISAC). Many organizations in this room are members of FS-ISAC, but I guess most of you are from the payments side and possibly do not have an IT relationship with them. So, Charles would like to introduce FS-ISAC.

Mr. Bretz: I will give a quick introduction of FS-ISAC. First, I want to thank many of you who are members; you are the reason we have this information sharing and have this organization. For you who are not familiar with FS-ISAC, we are a nonprofit formed in 1999 to protect the critical financial services sector from cyberattacks. We are owned by the financial services industry, so we are owned by the broker dealers, stock exchanges, card brands, payments processors that send transactions to the card brands, credit unions, banks and insurance companies. It is a financial services organization. We try to mitigate cybercrime from many different threat actors. After the 9/11 attack, our charter was expanded to protect against fiscal attack by sharing information. We process thousands of different threat indicators a month, sometimes thousands per day. I will get into how we are trying to adapt to that information flow, the speed of information. We have grown quite rapidly. We have 5,900 participating institutions. We have about 2,500 financial institutions bound by our operating rules, who are under nondisclosure, under contract to share their information under our operating rules.

A couple of years ago, our board of directors asked us to expand across the U.S. borders. So now we have members in Western Europe, Australia, Singapore and Japan. We are probably going to pick up some membership in South America very shortly. Again, it is in response to members like MasterCard, worldwide organizations that realized the threat is beyond the U.S. borders.

How do we share information? We have two security operations centers (SOC). Our original SOC is in suburban Washington, D.C. We also have a backup center under contract through IBM in Poland that allows us to expand the time zone coverage. Information goes both ways. It comes to the SOC and it flows out of the SOC. Government sources of information

are very important to us. We try to partner very closely with our government partners. And then there are private sources of information that we buy for our members using membership dues. Broad categories of member communications are information security, physical security, business continuity, fraud investigations and payment risk. What we find is probably 90 percent of the information comes from our members. The information from federal law enforcement and other sources is very important. But our members usually find out about the attacks first. That information comes in unfiltered. We try to coalesce that information and get it out to the membership. But the key to FS-ISAC is you as our members. Many of you work on the business side or on the payments side, and you are not an IT shop. When your organization joined FS-ISAC, it was probably from your IT chief information security officer, your CIO. That is the primary contact, but it has grown beyond that.

There are other ISACs, so there are other sectors. Nancy O'Malley is going to talk about some collaboration in the retail sector. Sandy Kennedy is going to talk about that too. For instance, FS-ISAC shares some information with other sectors. There is an aviation ISAC, oil and gas, there is a multistate ISAC that covers state to municipal government. Information could be shared between those sectors and FS-ISAC.

We have a number of information sharing and analysis tools. We keep secure repositories of documents. For instance, we have a playbook for denial of service attacks in its fourth edition. Those attacks sometimes come from state actors. Recently, some have been non-state criminal actors. Members have shared information on how to defend against denial of service attacks. That information is put in a secure portal, behind a lot of security. Many times members want information about how other members are reacting to particular threats, so we gather that with member surveys. Membership is so large and we have special interest groups, so we have different listservers for those groups. We do emergency calls when an event comes up. Sometimes we will have 900 or 1,000 members on a conference call to share the most recent information about a particular threat. We have semiannual meetings and they are very vibrant. We run three sessions a year on cyberattack against the payment processes. We run one for the United States and Canada, primarily against what we call the U.S. checking account. There is going to be one in Europe this year against current accounts. There also is one for the card processing group. The Federal Reserve has been very supportive, so we want to thank

the Fed for their support of those cyberexercises. Last year, 800 financial institutions in the United States and Canada participated in that exercise.

Now let me explain our traffic light protocol (TLP). When you share information under FS-ISAC operating rules, we color code the information. Red means restricted within a certain small group. That restriction is usually very short-lived. The small group works on the information and decides what is credible before pushing it out a bit more broadly. Yellow or amber means it can only be shared with FS-ISAC members. Green means it can be shared with the membership and partners, including our government partners. But when it goes to government sources, the Freedom of Information Act becomes applicable. White means it can be shared with everyone. We try to push out information at the lowest level possible to get the broadest distribution of information to protect the network.

We also have what we call circles of trust. Our membership is large with different groups that work on different issues. Groups will vet information, and if it is just for that group it might stay contained. But many times it goes out to a broader group. When that occurs, TLP is employed. For example, it might be TLP red within the cyberintel group or the threat intelligence council. And they are going to work on it and try to make it where the membership can understand, and then it might be pushed out very quickly with that analysis as amber to the 2,500 members who are under nondisclosure. And then if we can, we push it out green, which means it can be pushed out to all the support organizations that might be supporting your bank or your company.

I want to talk quickly about automation. One thing that has come up is the volume of information we push out at FS-ISAC is hard for our members to deal with. So that process is becoming automated. We have worked with the Department of Homeland Security (DHS) to develop a standard to speed up the process. The bad actors, the criminal actors and nation state actors can get into your organization quickly, and unfortunately, it takes a lot of time for those attacks to be discovered. There is a need to speed up the information, and the volume of information is so great our members asked us to find a way to automate it. Our members generously provided funding for a security automation solution. We are using a taxonomy developed by DHS, STIX and TAXII (Structured Threat Information Expression and Trusted Automated Exchange of Indicator Information), so we can have machine readable information that can be pushed out to your devices like

your firewalls, security management systems, your data integrity systems, and those types of things. That is what FS-ISAC does.

Mr. J. Williams: Thank you, Charles. Any questions from the audience on Charles' initial comments? I have one. It seems that over the last few years we have seen a change in the type of threat actors. We have seen it move from disorganized crime to transnational organized crime and state actors. How do you react to that?

Mr. Bretz: I will start with transnational organized crime. Those criminals are very sophisticated and their business can be very profitable. They are highly incented to attack our members. Because that business is profitable, they have a lot of resources. They can share resources and it just builds upon itself. That increases the need for collaboration. It is the same thing on the state side. A well-funded state actor has a lot of resources, and as you said in your opening comments, it is difficult for one financial institution to stand alone against the state actor. We need the members' information as well as our partnerships with government partners to help defend against that.

Mr. J. Williams: Thank you, Charles. Now Nancy O'Malley from the Payments Security Task Force is going to talk about how to secure cardholder present transactions.

Ms. O'Malley: Thank you so much. It is my pleasure to be here to represent some really interesting work. Yesterday, the presentation divided some of the work in the marketplace between public sector and private sector, and by way of characterizing this effort, it is purely private sector. But I am interested in finding out how we can take the work that has been done by this group and do more.

What is the Payments Security Task Force (PSTF)? There has been some information in the press; we would like to have more. PSTF is an initiative launched by MasterCard. Our CEO, Ajay Banga, was concerned about the progress toward migrating to EMV in the U.S. marketplace. As he encountered his counterparts and spoke with customers about their issues and concerns, he felt there was a need to foster a different level of collaboration at the most senior level in our marketplace in the payments security space. He launched this effort in February a year ago. The goal was to bring together c-suite executives from various organizations and to gain and secure their commitment to advancing solutions purely in the safety and security space. There was an initial meeting of the CEOs and they made a series

of commitments to be continuing participants. Those commitments were that they had to personally attend meetings and that they would expend company resources to advance initiatives the group collectively felt were the appropriate focus for the PSTF. It was an unusual and unprecedented activity. He reached out to his counterpart at Visa, who was glad to support this effort and join as an equal partner. That is how the PSTF was launched.

Let me talk about the structure of the task force and its focus. First was that we would have a senior executive steering committee, and if you can imagine bringing CEOs or c-suite executives from all the organizations, it was an interesting proposition—lots of strong opinions, lots of disagreement. But sharing and focusing on safety and security, and what we might do collectively to advance that was definitely a shared concern and a shared value. We also felt we needed a third-party manager to bring structure and appropriate balance because it probably was not going to work if MasterCard and Visa did that alone. We retained McKinsey to do that, and to foster that spirit of collaboration, to advance appropriate work streams and work efforts necessary to achieve our goals. Likewise, we appointed two individuals, one from MasterCard and one from Visa, my counterpart at Visa, Kim Lawrence and I. Together our role was to continue to advance the PSTF's day-to-day operations. Kim and I, together with McKinsey, are the project management office.

We said we need to put some structure and organization together. We asked what key things the PSTF needs to focus on that could allow us to make some real difference in the marketplace without getting bogged down in antitrust and other issues, which sometimes become obstacles to our collaboration in the industry. With the help of the steering committee, those were defined as tokenization and encryption, EMV (obviously that was the basis for the formation of this group in the first place), communications, and a group focused on the consumer experience. So, with each senior executive agreeing to provide resources, we had multiday workshops with technical individuals within their respective organizations who were in a position to make a difference and provide the input necessary to do the work.

In the tokenization/encryption space, we found, and I heard it yesterday in the presentations, there is a great deal of confusion in the marketplace about what tokenization is, how it is deployed, what the structure is today and what it needs to be in the future. And so that particular task force was

charged with developing a white paper to guide merchants, acquirers and issuers on how the technology should be used, and how they should make advances for their respective businesses and their respective markets. Of course, it cannot provide definitive answers to all use cases, but a series of use cases defined by these participants were designed to address how tokenization could be deployed in their specific markets and environments. Merchants, acquirers and issuers were engaged in these work streams.

EMV was where we started, and that was the history of the formation of this group, so a great deal of effort was then placed behind EMV. As that group formed, they learned a series of different things that needed to be done. First, there was a lot of confusion in the marketplace about where we were in our migration toward EMV. There were surveys that had been done, but none with regular cadence. They were all point of time. And so the participants in that particular work stream committed to contribute data. It is not 100 percent of the marketplace and it was never designed to be, but it provided a benchmark against which we could take these participants who represented 80 percent of the U.S. market from an issuing perspective, and measure their advancement of EMV from their perspective. Well, the measurement of EMV advancements and deployment from an issuer side does not really do us much good without also looking at the merchant perspective. Because there are so many merchants, it was impossible to effectively do a survey of 100 percent of the merchant community. Instead, it was decided the acquirers would work to provide data on what they had done to support the merchant community. Admittedly, it is very incomplete, but a good benchmark to measure, from a baseline perspective, the advancements of the deployment of terminals in particular.

Yet to come will be information on when we start to see chip-on-chip transactions. You can talk about the deployment of cards, the deployment of terminals, but it is really the enablement of terminals and then the traffic associated with chip-on-chip transactions that ultimately will start to give us a feel for how quickly we are advancing in the marketplace. Are we behind schedule, are we on schedule, are we accelerating? And although we can see that activity from a network standpoint, we really did not feel that just the network perspective alone would tell the full story. We are not there yet in the collection of all this data; we are not there yet in the publication of the data; but we are in process. Some might suggest we are a little late or behind the timeline, and that is probably a fair criticism. But the determination of this group was we have to start somewhere; we may

be behind the timeline but we need to start now and move forward. They are at a quarterly cadence to do just that.

Our communication work stream is the next interesting activity. The communication teams came in believing their goal was to talk to the industry about the PSTF's accomplishments. And to some extent that was the charge we gave them. However, we have quickly determined there are a host of communications issues around EMV and the market that needed to be tackled and the principal one was the consumer experience. We heard this loud and clear from the merchants who are participating. They had concerns about whether there would be a slowdown at the terminal, what their role would be, how much burden it would be to facilitate quick movement through the checkout line and other burdens to advance the work we were trying to do with EMV. What would be the merchant impact? That input was invaluable to the work that we wanted to do to overcome that particular issue. So, that interaction with senior officers from merchants who participated in the task force, and also a variety of different market segments, was really valuable to us.

The goal here was, and what our learnings were, that we needed to focus, to set aside our differences and find the pathway forward that could quickly allow us to make progress on advancing EMV. Another key element among these was the development of a value-added reseller qualification program. It is an interesting piece of work. It was designed to educate value-added resellers to play an important role in the marketplace to educate merchants on the value of EMV. More importantly, it discusses the implications of liability shift and what it could mean to them and their businesses if they do not get on board and work to advance the adoption of EMV in their businesses. That program was designed to streamline and eliminate obstacles the industry had created toward getting merchants into the program quickly.

Then finally, the last one is the launch of *http://gochipcard.com*. That is very recent. It is a consumer education effort done in conjunction with the EMV Migration Forum. I am sure many of you are participants and are aware of the work of the EMV Forum. All of the work of the PSTF was designed to support and tackle those issues that the EMV Forum had not been able to do, and to supplement their efforts and was done in coordination with them.

So finally, the PSTF's accomplishments; we have twice published quarterly issuer and acquirer EMV survey results, published and distributed

a payments security roadmap white paper, launched a U.S. EMV Value Added Reseller Qualification Program and launched the *http://gochipcard.com* education microsite. We believe these accomplishments demonstrate the commitment of our marketplace to work together, and how we can be effective when we determine we need to do so. It also demonstrates that we can find common ground to advance work that is critical to our marketplace. We built an integrated roadmap, which has provided great guidance in what to invest, when to invest and how to invest. We have overcome some real barriers and we are providing great data into the marketplace to inform decision-making by these key stakeholders and participants. And we are going to leverage this group to identify and anticipate issues in other areas that impact safety and security going forward.

Mr. J. Williams: Very interesting, the breadth of the collaboration and the number of different stakeholders you have involved. Any questions from the audience?

Mr. Santana: Nancy, you mentioned you have been running this Payments Security Task Force for over a year. What are some of the key challenges and lessons learned you could share with the Secure Payments Task Force as we embark on the same journey?

Ms. O'Malley: One key lesson from this is that at the outset, although this organization does not have a legal structure and it does not have a charter, it really is the commitment of the participants to build and foster collaboration. Our ability to do that, and the success that was derived from this work. We had folks with very different viewpoints, but we tackled some key initial things that allowed us to build trust between the participants and to demonstrate to each other how we can collaborate to move things forward. I think what is really exciting about the Secure Payments Task Force is this marriage of the public and private partnership, because there is only so much we can do in the private industry world to advance some of these really important initiatives. But when we marry that with the opportunity to work with the Fed and to tap into their resources and insight, to advance this and provide some structure, I think it really is an opportunity to take some of the work we have done and move it to the next level. So I would say, start small, find those things which we can tackle quickly together, agree on the spaces within which to collaborate, and what you are not going to talk about to ensure you continue to advance and do not get bogged down in some of the political issues that clearly surround some of these things. That would be my advice.

Mr. J. Williams: I would like to hand the presentation over to Sandy Kennedy from the Merchant Financial Services Cybersecurity Partnership. There is going to be more of a merchant perspective on these problems.

Ms. Kennedy: Good morning, everyone. There is a lot of attention paid to the conflict between retailers, card networks and banks. And while there remain significant disagreements and challenges, we really have been encouraged by the amount of collaborations over the last 18 months. Obviously, with the major breach that occurred with one of our members in December 2013, the Retail Industry Leaders Association (RILA) board of directors, which at the time was chaired by the CEO of Target, saw a necessity for us to come up with a plan to move forward in collaboration. The CEOs clearly saw the payments system as an ecosystem, and there was no way we could move forward in a collaborative way unless we included everyone in that ecosystem. So they gave us direction, and it was very clear. They said to collaborate where possible, only fight if we must.

The example I am going to talk about is how we acted on this direction immediately, and it was with the formation of the Merchant Financial Services Cybersecurity Partnership. This partnership started when I reached out to Tim Pawlenty at the Financial Services Roundtable and found we were likeminded on a lot of issues. We had the opportunity to agree on a number of things. There were going to be things we disagree about, but we were going to find those areas where there was agreement, and try and move forward collectively. So together, with an outstanding team that he had, and the RILA team, we pulled together 19 associations representing the financial services and retail industries from all different areas, sizes and formats. They were all at the table. And from that, we worked on five key areas. I think ultimately the dialogue exceeded most of our expectations, and in the end important relationships were forged. I think we were able to talk about areas in which we disagreed in a way that was productive. The challenge now is that the partnership has come to an end. It was never intended to be a permanent body, but it is important that collaboration continue, so we are going to look for ways to do that, and support and push that forward.

Based on our experience, there are five major areas where collaboration across the payments ecosystem is important. I would give high marks to two that we were involved in, a mixed score to one and probably a failing grade on two. The one I will give really high marks to is cyberthreat

information sharing. The ability to share with others in as close to real time as possible, information about attacks faced and how they can be defeated, is one of the most valuable tools in the retail cybersecurity toolbox. Through this partnership, we learned so much from the financial institutions that were involved, FS-ISAC and other organizations. With their help, knowledge and experiences we were able to put together a Retail Cyber Intelligence Sharing Center. This is a separate organization that will house the retail ISAC. It is almost a year old and I think recently there was a formal relationship formed with the FS-ISAC, which will be extremely beneficial to both sectors.

The area where I also would give us OK marks is the payments ecosystem in terms of long-term payments and our view on that. There is a tremendous opportunity right now in retail in terms of how we look at omni-channel mobility, the digital world. There are so many opportunities for how people are going to shop now and in the future. We had a really good dialogue across all the industries on what we need to plan for this next generation of threats and technologies. Tokenization was an important part of this discussion, and while tokenization is still a ways from being able to address card security in the near term, it has great potential in the long term. We hope the collaboration, development and eventually how it deploys continue.

The area where I give us mixed results was in legislation. Policymakers at all levels, state and federal, were looking at ways to reduce cyberattacks. The partnership really did help to inhibit, deter and distract lawmakers who were looking to do kneejerk reactions to some of the cybersecurity breaches that occurred in the retail industry. In working with the financial institutions, we jointly called on Congress to pass legislation on sharing cyberinformation, which provided liability protections in our sharing environments. The House of Representatives has passed this legislation, and we are awaiting action in the Senate. What we disagreed on was what data security legislation should look like. Banks want laws narrowly written for banks to be applied to the rest of the economy. Retailers have endorsed added standards based on more than a decade of enforcement by the Federal Trade Commission. We are still working on that and hoping we can come to an agreement.

An area where we have had challenges and straight out disagreements—I know Liz Garner talked about some of this yesterday—is standard setting.

Retailers have long been frustrated with the process with PCI. We have never had a seat at the table, never been asked for input, and so much of what PCI dictates affects how we operate as retailers. We think we have a meaningful perspective and input and would like to be part of that process as we move forward.

The area of greatest concern and disagreement is how to improve security on more than 1.2 billion cards in circulation. But before I get into the details of that disagreement, it is important to step back and look at the bigger picture. The threat we face from cybercriminals is enormous and evolving. They are tenacious and sophisticated. Given the scale of that threat, we must employ a variety of tactics to be successful. Further, it is our perspective that the important work we are doing to harden systems and share threat information is limited by one undeniable truth. Criminals know economics. They know how to look for information. They are tenacious at looking for information that passes through our point-of-sale terminals, and information that we capture. And it does not matter how thick or how high we build the walls, the bad guys are motivated to find a way over, under, or through. But while we are hardening these defenses, we need to focus intensely on devaluing the data, removing the incentive for cybercriminals to lodge these attacks in the first place. When Europe grappled with these issues a decade ago, the solution they employed was chip and PIN. As a result, we saw substantial reduction in fraud. Since then, nearly every other industrial country has followed Europe's lead, deploying chip and PIN. Not surprisingly, fraud, like water, flows to the path of least resistance. That is why fraud migrated to the United States. As we all know the payments ecosystem is in the process of migrating to EMV. Unfortunately, we are not moving to chip and PIN like the rest of the world. Instead, we are moving to chip and signature. With this migration, the United States will sadly retain its position of being the path of least resistance.

Retailers believe that we need, and have an obligation, to walk and chew gum at the same time when it comes to payments security. We must migrate to the best security technology on the 1.2 billion cards in circulation, and continue to work together to ensure our customers' security with new technologies and shopping opportunities.

Mr. J. Williams: As part of how we are dealing with innovative criminals, where can you innovate to try and protect your businesses against them? How can you drive and promote that?

Ms. Kennedy: The collaboration provides great insights into leading practices. We had been patiently selling things and really did not consider ourselves technology companies, which is what we are. We have become technology companies. And so we had to change our mindset and think differently. Again, through the working groups, there was a lot of sharing of leading practices, areas that our sites had never even thought about. From that standpoint, that allowed us to leap forward in our learning curve in this area.

Mr. J. Williams: Thank you. I would like to hand it over to Liz Votaw, who is going to talk about how we ensure exactly who we are allowing through the walls of our castle.

Ms. Votaw: Good morning. I am from Bank of America, where I lead and develop strategy for authentication across all the different channels in the consumer bank. But I am here today as a member of the board of directors for the Fast IDentity Online (FIDO) Alliance. I am not going to be able to answer questions about Bank of America, but I am happy to explain what the FIDO Alliance is and answer those questions. FIDO is different from other collaborations that have been spoken about, but there are similarities. What makes it different is that FIDO is not a payment-specific collaboration. Our focus is on authentication, and helping companies throughout the authentication ecosystem ensure that their implementations of authentication technology are safe and secure for consumers and for the companies relying on them.

When you think about the authentication landscape today, there is a lot of looking for that silver bullet. Everybody understands there are lots of problems in authentication, and a lot of people are running quickly toward the new silver bullet of biometrics. I am going to talk about the key principles FIDO lives by and says if you are going to move to biometrics or some other kind of authentication in a mobile device, make sure not to make the problem worse by following some of the same problems experienced with passwords.

Who is the FIDO Alliance? If you look at the board of directors, what you see is a true cross section of every type of company involved in authentication. Similar to some other collaborations, you see representations from many players in the payments landscape, but they are not here specifically only to focus on payments, but also to focus on access in any way to any personal or private data, some of which may or may not be financial. The

healthcare industry is also part of the FIDO Alliance and we are hoping it becomes an even broader opportunity. There is a lot of commitment across the technology and finance spaces in the FIDO Alliance.

What is the FIDO Alliance's mission? Many people have this image of a dog. Take that out of the picture completely. A lot of people also have this image that FIDO is a product. It is not a product. There is no profit in this equation. It is not a big database where all of the biometric prints sit. I have heard everything under the sun about, "Oh, you know, talk to FIDO about that," but that is not what FIDO is about. What FIDO is about is developing technology specifications that companies can implement across the spectrum. So you will see that it gets built into the handheld device itself, built into the servers on the relying party side and it employs this specification across the board with a certification process. There is an operating adoption program, so we have the whole marketing arm of the FIDO Alliance to ensure that this is truly getting adopted across the landscape. And then we are going to pursue formal standardization, as was talked about yesterday. Right now we really are just specifications until we go through some of the broader global standardization bodies.

As I mentioned before, the FIDO Alliance was formed to solve this ugly, ugly password problem. And in your world, it would probably be more PIN and authorization and things like that, but when you think about the whole ecosystem, everything comes back to these critical secrets—passwords, PINs, data, etc. We know we have this awful problem; we know what happens. You are living it every day. A lot of people try to solve for that problem by taking a different approach and saying, OK, how about going to one-time passcodes, and solving the problem that way. While one-time passcodes are certainly an improvement on passcodes, they certainly are not the ideal solution for various reasons many people have experienced themselves. They are not that user-friendly. You have to sit and wait for your little code to come. If it is a physical token that you have to use, and you have to type in a code, you end up with a key like a janitor's keychain with all the little tokens hanging off of it. It gets confusing for customers. Which code is this, and when am I getting it, and unfortunately, it is still phishable. We have seen in the last year that more and more of those things are getting phished as well as intercepted. So, one-time passcodes are not the answer. Passcodes are not the answer. What is the answer?

What the FIDO Alliance says is, "We need a new model, a new paradigm for how we view passwords, especially if we are going to move into this space where we are relying more on biometrics." When you look at and try to analyze some of the key problems with passwords, there are consumer issues with, "I have to remember it, and it needs to alphanumeric and include my gardener's middle initial and I do not know what it is." It is awful and everyone understands that. But when you look at the way it works, you have a consumer taking that very critical piece of data and sending it across the wire to a server. There is a lot of vulnerability. You can interrupt that online arrow any number of ways if you are a bad guy, or you can just target—no pun intended—the server. So when you look at the new paradigm, in many ways similar to tokenization, what it says is devalue all that data and turn it into a cryptographic key environment. What you are talking about there is that the consumer interacts with their device. This could be a mobile device or a laptop. You are interacting with that device and proving to it who you are using a biometric, PIN, or something else. And then that device generates a private key and stores it in the secure aspect of that device. That private key then speaks to a public key on the server side so then the authentication is really happening, the credential is really those keys and no longer the biometric. Instead of looking at biometrics as, oh, all I have to worry about if I am a big company like Bank of America and I want to use biometrics, I need to make sure that the false accept rate and the false reject rate are where I want them to be. Most banks are not in the business of understanding that business. That is not their core competency. But being able to say, OK, I have a key on my server, and it can only speak to this unique key on this device, we can certainly understand that a lot better. It actually takes a lot of pressure off making sure every single biometric is at the false accept rate that you need, and you can start to evaluate the risk you are using to determine how much security you really need out of this device.

When you look at what FIDO offers, it is a standard or a set of specifications that can solve for two different business or use cases. One is we want to get rid of the password and replace it with some sort of device-centered biometric. FIDO has a standard for that. Or, not all devices are going to have biometric capabilities, so how can I still use the FIDO standard? I can still keep my password environment, but instead of the one-time passcode I can layer on top of it a universal token. In some cases that is a physical token; in others it will be built into a device so it can be incorporated there.

When you look at the FIDO Alliance's key principles and you start to think about implementations across the board, if you follow these key principles, then you are closer to being in conformance with FIDO than if you did not. So, no third party in the protocol, no secrets on the server side. Think about the problems we have gotten ourselves into. To this point, it has been breach, breach, breach, breach because we have secrets that are breachable and we should not be so arrogant as to think we can perfectly secure all of that. Just like you have been saying about devaluing the data, do not take your favorite thing that you do not want someone to have, and leave it in a jewelry box for someone to break into. Only leave your crappy stuff that nobody wants in there. Leave nothing there that is worth taking and you will be in a much better position. Biometric data creep people out. They do not want it in the hands of big bad banks, others and government. They want to keep it close. So, keep it in the device, so it does not go anywhere and what happens to their biometric is between the consumer and the device. That means that if I am a bad guy and I want to remotely steal fingerprints, I have a lot of work to do. I have to fly to the United States and start stealing 2 million devices, instead of sitting in my hotel room in, we will not name the country, opening my laptop and starting to hack.

No linkability between services, no linkability between accounts. If I have a FIDO-certified device, and I will talk about what that means, and I enroll my device with PayPal, and then also with Google—just because Google and PayPal accept FIDO does not mean they share any information about you—it is completely separate. Look at what the FIDO Alliance has accomplished, similar to the collaborations we have talked about. The public specifications, you can go to the website today and pull off that specification. It was publicized in December and companies have been building to that. In 2014, we saw adoption by some key players, PayPal, Alibaba and Google. This is clearly a global group, not just a U.S.-focused group. Today, if you are a Google customer, sign up for two-factor verification, two-step verification, it will give you a choice. You can use a one-time password. It will send you the SMS, or you can go to Amazon and buy a little token. And you put it in your USB port and it functions as your second factor. You do not have to put in any codes. You just put it in your USB port. So, someone would have to get your password and your device because this token only works in that device. In 2015, we saw more momentum with Microsoft announcing that Windows 10 would support FIDO. Qualcomm has said their chips will now support FIDO in devices where they have

been placed. Google has expanded its use of the token to Google at Work. And NTT Docomo, the largest Japanese wireless carrier, has announced a whole line of FIDO-certified devices. There are a bunch of other companies that have gotten FIDO certified. And perhaps of most interest, it now is a public-private partnership because the government is joining the FIDO Alliance. The National Institute of Standards and Technology just joined, and the U.K. government just joined. So it is your turn to join, and ask me any questions that you have about the FIDO Alliance.

Mr. J. Williams: Any questions for Liz?

Mr. Horwedel: My question is that given the fact that we are about to see a huge increase in e-commerce fraud as a result of moving to EMV, and the merchants are going to bear almost all the associated costs, should we pay any attention to resurrecting 3D Secure, which was a very poorly designed product in the first place that resulted in gross abandonment of purchases during the process. I understand it has been redesigned. Should we go down that path, or can we expect something to materialize, or has it already materialized, that we should move to rather than fooling around anymore with 3D Secure?

Ms. Votaw: I cannot really comment on 3D Secure, but I can say that there are Web solutions as well as mobile device solutions that FIDO offers. As I mentioned, Microsoft's Windows 10 opportunity means that if you go on the new browser Microsoft is introducing—Microsoft Edge—when you interact with any of those companies on the Web, if any of them accept a FIDO authentication through Microsoft Windows, then you will be in a much better situation from a security perspective. I think the future is very bright for innovation and technology, and really what the FIDO Alliance is saying is go down all of those paths, but do it smart. Do it according to a standard that everyone can sign up for.

Mr. Horwedel: And correct me if I am wrong. You are also saying that you are focused in an open standards environment rather than a proprietary standards environment. Is that correct?

Ms. Votaw: Completely open source, yes. The only thing you pay for in this environment is if you want to say that you are FIDO certified, you go through certification and pay a small fee. And then to implement FIDO, it is open source, but there are vendors you can hire to do the implementation, so you can buy the server from the server vendor. If you are a

merchant, and you want to have an e-commerce site and be able to accept FIDO devices, you can hire a FIDO vendor or you can build it yourself. It is open source.

Mr. J. Williams: Thank you for the question. One thing that strikes me listening to the panelists is that to be successful in any of these collaborations, it is very important to define the scope and focus on those deliverables. How do you measure effectiveness or whether you have succeeded? Charles?

Mr. Bretz: That is a good question and I think there are a lot of metrics out there, and of course, more metrics that we could collect on those. It is a challenge for us on the cybersecurity side. You see these published numbers—$10 billion are lost or $1 billion are lost, and it is done by an estimate by some outside firm, and it is not really tallied where we would be audited and have audited numbers. Back to the card brands, they certainly can measure chip-to-chip transactions; they can measure the fraud as a percentage of payment volume and those types of things. We are going to have to look back to card brands. NACHA collects statistics in that area. What we are going to have to do is look to those folks in the payments area that collect that data. Certainly the Federal Reserve does a study every couple of years on the losses, and so those are the measurements I would want to go back to rather than the headlines we sometimes see in the trade press.

Mr. J. Williams: So you are looking at a financial metric?

Mr. Bretz: Right.

Mr. J. Williams: Nancy, what does the success look like for you?

Ms. O'Malley: The objective measures certainly are an important aspect, and that is why one of the essential things the PSTF felt was important to contribute was data on migration to EMV. We are getting ready also to launch surveys about utilization of tokenization as well as encryption because it is really the suite of these technologies that will work together to create a safer environment. Those are the objective things. But probably the more important things are the subjective things, the partnerships being built, the networking that is occurring to share thought leadership. FS-ISAC certainly does that in the cyberspace, but in the payment ecosystem that historically has not happened between competitors. Of course, we have to be very careful and monitor the space in which we do that, but in the security space, it probably is the easiest place for us to come together and

collaborate. So, we are measuring success by publication of thought leadership papers, the feedback we receive, the requests for more information and data, tasks from our executive committee, what we need to continue to do or tackle next. Those are what we are looking to as subjective measures of the progress being made and our success.

Mr. J. Williams: So it sounds like you are looking at the metrics and working that out, how they are evolving, to the things that you are doing to try and secure the rest of the payments system?

Ms. O'Malley: Absolutely.

Mr. J. Williams: Sandy?

Ms. Kennedy: We do not have specific metrics other than the same commitment we had from all the associations involved over an eight or nine month period. We had literally hundreds of hours of conference calls, in-person meetings, and that is the same commitment and involvement from both the retailers and the financial services and other players in the ecosystem. It speaks for itself that we had that kind of participation and that we have ongoing conversations, less formal perhaps, but ongoing partnerships and conversations that are occurring and understanding that we have a commitment to a shared customer that we need to protect.

Ms. Votaw: My answer is easy. Adoption. That is how it is measured. The more companies that say we are going to take the time and build security into our whole process, the more successful FIDO will be and the more likely it will be to spread across sectors beyond financial into healthcare and other areas that desperately need help, and consumer behavior. If consumers start to really adopt biometrics as a way of life, but feel comfortable about it and feel protected, then FIDO has been successful.

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.