General Discussion

Role of Government in Payments System Security

Mr. Werkema: Thank you. Have the responses spurred any questions from our conference participants?

Ms. George: I want to thank each panelist for the perspective you brought on the issues we have been discussing for the last day and a half. Coen, you made a comment that I found interesting, which is we tend to think about technology when we focus on these issues instead of the importance of culture. My question for each of you, but I am happy to hear Coen elaborate on this, is what role do you think public authorities play in influencing culture? Is that primarily through education, regulation? What, in your experience, would a public authority bring to that?

Mr. Voormeulen: That is a difficult one. What I can imagine is that what helps best is to make people aware of it. We bring parties together, including a security company in the Netherlands called Fox-IT, which is very experienced. We bring them together to talk, to let *them* talk, to share these kinds of things with financial institutions and financial market infrastructures. Then, when the federal institutions hear it, they probably recognize something of it and can apply it. But you cannot impose cultural things. That is the difficult thing. The only thing possible is to make everybody aware by sharing practices.

Mr. Mukherjee: What I could add is that we find it is very difficult to prescribe culture. As Coen said, one way we handle this is by talking about it, but also by framing our output, not narrowly in cybersecurity per se, but more about enterprise risk management. So, when we encourage certain frameworks, like the National Institute of Standards and Technology (NIST) framework, or we engage with the private sector on cyber and we talk about it, it really is more about organizational and risk resiliency, overall business continuity, and we talk a lot about governance in that

context. There is no precise way to get a culture necessarily, but by framing the issues, the questions, and then the solutions that we would encourage in a broader milieu and with governance as an important part of that, that is how we indirectly try to get at it.

Mr. Tsiliberdis: What we emphasize is trust. We try to build trust among the different participants. We want to assure them that by building on this trust among themselves, they will be able to adopt technologies that will make them compatible, not enter into competitive fields. We try to help them see how this communication can be done from all the different actors by using technologies which are interoperable.

Mr. Santhana: I have a question for Anjan. We work a lot with federal and state governments. We find there is a big difference in terms of cybersecurity, enterprise, fraud management and even in the payments environment, payments modernization. There seems to be no set standard, no task force that helps pull the various state government entities to follow what the federal government is trying to do. Is there any initiative, anything going on now that you can share?

Mr. Mukherjee: It is a tricky one because states are independent. Each has its own, as you know in dealing with them, IT network and system and that legacy of independence. We have very much noted the issue you have outlined. There is no specific broad initiative, to directly answer your question, in the works to address this issue for many reasons. There are impediments in place for the federal government to try to standardize this issue or approach it at the state level. We are limited in what we can do, but we can talk about it. We have convened with certain leaders in state government to discuss the issue. We encourage state governments to join the Financial Services Information Sharing Analysis Center (FS-ISAC). But this is really more of a moral-suasion process, where we try to rope them into our effort, make them understand how we are approaching the issue and encourage them to try to look at it the same way.

Ms. Fine: All of you in your remarks touched in one way or another on both strategies of collaboration and moral suasion, best practices, education, as well as regulation, legislative approaches. I am wondering if you can speak about that balance, and where you found regulation to be most effective or necessary to preserve the safety of the system versus the other strategies you have talked about.

Mr. Voormeulen: Again, That is a difficult point because it is a balancing act. One characteristic of cyberresilience is that when you go deeper into the technicalities, everything you would put into legislation probably will be outdated before it is out. You need to be more high level in legislation to make sure it is still relevant next year and the year after because of the quick developments in cyberattacks. That makes best practices the most effective way in the short term to pass on to all the relevant parties, because they can be updated relatively quickly. But at the same time, a legislative framework that stays high level but aims at the goals and not how to get there can be very useful to exchanging these best practices.

Mr. Mukherjee: Yes, I would say these various efforts are complementary. More of all is better. There are situations where there is some potential conflict, but generally we think those are manageable and relatively minor. To take information sharing as an example, Treasury just joined FS-ISAC. We encourage financial institutions to join FS-ISAC, which has something like 5,500 members. The financial services industry is well out ahead with this ethos of information sharing, as evidenced by the success of FS-ISAC. Even though we are Treasury and the government, we promote adoption of this model by other industries—healthcare, energy and so on. But if you look at the president's legislation on information sharing, it is wholly consistent with that sort of non-legislative approach that we have taken and it is just meant to provide additional impetus. As Coen just said, it is not technical, it is not detailed. It is meant to be a broader framework. In some ways, we are already working in that framework without the legislation, but we think the legislation has some very important elements that will accelerate what we are doing through liability protections, and other things, that will encourage not just the financial services industry, but participants in other industries, to adopt an aggressive information sharing regime.

So, I think that there is not necessarily, kind of the way you framed it, a conflict. We think these are complementary and more is better.

Mr. Tsiliberdis: I would like to add that the reason we move from moral suasion to regulation is because we have seen that some entities were not fast enough in implementing some of the policies, some of the recommendations, some of the requirements that we have highlighted with the previously non-binding recommendations that we were giving to them. So, to establish, to raise the bar in terms of efficiency and security, we have decided within the euro area and the Eurosystem, to convert some

specific recommendations into regulations. This is what we have done for the large-value payments systems and what we also are doing with the retail payments systems. Soon we will be doing this with the retail payment instruments, with the Payment Systems Directive once it comes into force, with other recommendations that will be issued by the European Banking Association Authority in the field of retail payment instruments.

Mr. Werkema: If I could just follow up on that, Chris. So, your framework had moral suasion, regulation, but then you also addressed the operate aspect with the European Central Bank (ECB). So, what would lead the ECB to stand up or enhance capability on the operate side versus collaboration, coordination, moral suasion, and regulation? What would lead to an operator capacity?

Mr. Tsiliberdis: As you mentioned, the area the ECB mainly has stepped in was the large value payments systems. And last Monday we went live with a new security infrastructure. It is where we want to ensure that services that are critical and important in the euro area, and for which we do not see the solution is already available in the market, then, in that case, we try to step in and implement these solutions. Sometimes of course, we will see some kind of reaction from a service provider that they know we are entering that field and ask why we are implementing something. But this is because we want to ensure that the level of service provided to the citizens and various financial institutions is appropriate. For that reason, we step in as operators for these specific systems. We have not done it yet. But in terms of the ECB in the telepayment systems or our telepayment instruments, I know the central banks in the euro area, which are active in this field, have implemented their own solutions.

Mr. Werkema: At the ECB level, your focus is on wholesale systemic systems?

Mr. Tsiliberdis: Yes.

Mr. Werkema: Other questions?

Mr. Moore: You all were talking primarily about public sector initiatives to improve payment system security, and each involved engaging the private sector. But this morning, we heard about several initiatives that were initiated and led by the private sector, and I am wondering what role, if any, do you think public authorities have in supporting or engaging with these private sector led initiatives?

Mr. Mukherjee: Maybe I can take that one, and maybe I will shift a bit the answer, to not answer your question specifically but to talk about a different scenario, which is where the public sector has created its own programs and initiatives, divorced from the private sector as a way to encourage objectives here. I mentioned one in my opening remarks, which was an executive order the president issued in October 2014. It is the Buy Secure Initiative, which has many elements. One is to move all government-issued cards to EMV technology. This is a way to harness the government's purchasing power to try to drive and encourage change and enhance technology in our system. If you look at recipients of federal benefits who are unbanked, the idea would be to populate prepaid cards with their benefits and the program we have set up is called Direct Express. It has about 2.5 million people on it. Those cards are populated with about $2 billion worth of benefits every month. We as a government, independent of what the private sector is doing, have decided to encourage—and we talked during this conference about how the United States is far behind on EMV chip and PIN—to prime the pump in that way. Similarly, all of the government's payment card terminals will be upgraded. There are about 3,200 terminals across 52 different agencies. Our target is by the end of September of this year to have all those terminals upgraded. We are on target. We are finishing phase one with about 19 agencies, and there are almost 120 million annual transactions that go through that network. By the way, that hardware also will be near-field-communication (NFC) enabled. So, eventually the Apple Pay, Samsung Pay and Google Wallets of the world could—not that they will work day one—but could work because the hardware at least will be enabled to do that. So, it is not exactly what you asked, but I think it was important not only to talk about the private sector initiatives, but the fact that there are entirely public sector initiatives that also are meant to accelerate the pace of improving the security of our payments system.

Mr. Voormeulen: Maybe I can mention one example. In the Netherlands, we have a big group, a Retail Payments Board, which is chaired by the central bank. That is a broad group in terms of banks that are represented, retailers, consumers, but also disability awareness organizations for instance that have an interest in how user-friendly or what kind of retail payment devices are used. There are all kinds of sectors, with about 30-40 people around the table. Whenever there is an initiative or the start of an initiative in the private sector, it will come across that table. What we do then is to try to stimulate it, help it, sometimes a private sector initiative

needs competitors around the table. They find it difficult to agree on how to take it a step further, and then they need a neutral party, and then we can step in as a central bank or as this more societal organization to take the initiative further. So, everything more or less comes together on that table, and can be moved ahead in the best possible way.

Mr. Tsiliberdis: And just to complement what they have in the Netherlands. At the European level, we also have a Retail Payments Board, where we bring together representatives from the various service providers, financial institutions, infrastructures, and we discuss issues related to standardization and market integration in this field. We also actively involve market groups, where they discuss all these issues. For that reason, whenever we make a recommendation, when we make partner recommendations concerning the security of Internet payments, we will always take under consideration what has been developed by the market and try not to reinvent the wheel.

Mr. Werkema: I would also comment from a Federal Reserve perspective, that we have Strategies for Improving the U.S. Payments System. I have a leadership role there, as do others in this room. Our objective is to guide and support the industry as it moves forward in a couple of key areas. One is faster. One is security. Many people in this room are involved in our efforts. But the intent is not to duplicate or replicate what is being done in these private sector initiatives, but to complement, support, and maybe be an additive in our benefit there.

Ms. Garner: A quick question for Treasury. We are very supportive of government efforts to move the ball forward quicker on EMV, and particularly EMV and PIN transactions. But you mentioned merchant reterminalization. Even though you are going to have NFC capabilities, are merchants going to be required to turn on that NFC capability on those terminals?

Mr. Mukherjee: No. At the moment there is no arrangement to enable the NFC technology. In the future, that may change. There are conversations with some of the players that I mentioned earlier, but the answer is no.

Mr. Marshall: Just a question for Anjan. One of our concerns is the incidence of identity theft, and one of the best ways of stopping identity theft is to validate Social Security numbers. But weirdly, we are unable to do that in the United States in the Social Security Administration. So, we have to use private solutions that are not comprehensive. It particularly affects

the underserved. In some cases, we are unable to approve people without credit because we are unable to verify the Social Security number. Is there anything that you can do to solve that for us?

Mr. Mukherjee: OK. Let me take that away and come back to you. I had not heard that from you all before, so I do not have an answer. But it is an interesting question.

Mr. Santhana: Question for Anjan. It is very interesting to hear about the EMV initiative, prepaid debit initiative. However, as a government entity, you have to support the lowest common denominator at all times, and that is what we have heard every time we speak to a government agency. So, you are going to be on the payments acceptance side and on the disbursement side supporting checks until the last check transacts through the payments system. And you have to maintain these inefficiencies. So there are going to be complications in terms of cybercriminals focusing on the legacy systems. What is the plan; what is the thought?

Mr. Mukherjee: That is a great point. It is something we are very focused on. As I mentioned in my opening comments, when one is transitioning from a legacy system and upgrading a system, that often exposes vulnerability. I cannot get into the details about that, but I can tell you generally we are focused on it. Our plan is a mix of technological approach or solution to make sure that again we are adhering to our own mantra of optimizing baseline protection and best practices, recognizing we have systems in transition. And then also as we were talking about earlier, a cultural approach as well. It is a combination of those two things. We are aware that we have multiple, sometimes competing systems and we do have to support all methods of payment that run through our system. But the example I was talking about earlier is really more of a tip of the spear thing. That is to help encourage the private sector to move in a certain direction.

Ms. Padmanabhan: To follow up on Vernon Marshall's question, this is also a question for Anjan. For non-credit application, like for typical deposit applications, we still need to collect a Social Security number and verify it against those databases. However, dealing with many of the underbanked and unbanked, as well as individuals who do not want to provide their Social Security number online for understandable security reasons, that is a pretty big obstacle that issuers are facing. Is there any way to interpret the Bank Secrecy Act that does not require banks to collect

Social Security?

Mr. Mukherjee: That is a good question. Like the other Social Security question, it is not something that I have studied, so unfortunately I cannot give you an answer.

Mr. Werkema: Does anyone in the audience have a suggestion there? OK, Kelly, we will turn the floor back to you.

Mr. Dubbert: Please join me in thanking Gordon and the panelists.