

Role of Government in Payments System Security

Moderator: Gordon Werkema

Mr. Werkema: I have a few opening remarks and then we will turn to our presenters. When the conference began, Governor Powell stated important goals of the Federal Reserve in retail payments: strong security, high public confidence and responsiveness to evolving threats. As we have heard throughout the last two days, private market incentives drive payment providers to work hard in securing payments. Our first session highlighted various features of the modern payments system that may make private sector efforts alone insufficient to attain a socially beneficial level of payments security. As you know, payments are processed in networks involving many participants, and that makes coordination vital to security. Recent trends add to the challenge. In the last 15 years, payment processing in the United States has become overwhelmingly electronic. In 2000, just over 40 percent of noncash retail payments were initiated and processed electronically. In 2012, 85 percent were initiated electronically, but virtually 100 percent were ultimately processed electronically. Endpoints where payments can be made are exploding in the United States and throughout the globe. Merchants that accept card payments in the United States are above 10 million. Access to the Internet in 2013 witnessed 116 million households, and interestingly 64 percent used tablet computers. Nonbanks have been the leaders in developing new methods of making payments, especially in the online and mobile payment areas. E-commerce sales reached \$75 billion in the first quarter 2015, for a record 7 percent of total retail sales. Nonbank payment providers set a record for startup funding in 2014 at \$2.23 billion; but with \$720 million in startup funding in the first quarter of 2015 alone, that record will likely be broken this year.

While these are U.S. trends, we believe they serve to illustrate how challenging securing payments and transaction data more broadly has become. As a consequence, there may be room for enhanced public policy toward security.

This final session will explore the role government may take in promoting payments security. So, contributing to our discussion today, I would like to introduce our panelists. We have Chrissanthos Tsiliberdis, and he says I can call him Chris. He is a senior market infrastructure expert at the European Central Bank (ECB). He is responsible for operational risk oversight and policy issues. Importantly, he was involved in drafting the Eurosystem oversight policies on business continuity for systemically important payments systems, and he has represented the ECB and various working groups including those involving cyberresiliency. Next to him is Coen Voormeulen, director of the Cash and Payments Division at De Nederlandsche Bank. He importantly is co-chair of the Bank for International Settlements Working Group for Cyber Resilience. Lastly, we have Anjan Mukherjee, counselor to the secretary and deputy assistant secretary for financial institutions at the U.S. Department of the Treasury. Among his roles, he oversees the Office of Financial Institution Policy, the Office of Critical Infrastructure Protection and the Federal Insurance Office.

In their respective roles, these three panelists have been involved in policy initiatives related to deterring payment fraud and/or improving cybersecurity. We hope this session sparks questions and dialogue. Initially, I am going to turn to Chris. He is going to give initial remarks, and then we will ask some clarifying questions and then move on to the other panelists.

Mr. Tsiliberdis: Good morning, everybody. I would like to thank the Federal Reserve Bank of Kansas City for inviting the European Central Bank to express the views of the Eurosystem at this conference.

The main objective of the central banks in Europe is to ensure that the financial market infrastructures are safe and efficient, which is a precondition for doing three things. First, we would like to contribute to financial stability. Second, we would like to implement monetary policy. And third, we want to ensure and maintain public confidence in the currency. When we look into financial market infrastructure, we do not oversee differently the large-value payment systems and the retail payments systems. For that reason, maintaining public confidence in the retail payment systems and retail payment instruments is very important.

To maintain public confidence, the task for the central banks and the other regulators is threefold. It is to keep their approaches flexible enough to accommodate the pace of innovation, to ensure fair competition among

actors and to require that service providers implement adequate minimum security requirements. Accordingly, we have been actively monitoring what the market has been doing all these years. Initially, we had a very passive role in this, monitoring the market initiatives and how they were doing in order to sustain the efficiency and safety of the instruments they were providing to the market.

But we realized this was not very successful in some cases. So, we stepped in and started introducing new standards. We started introducing new recommendations, for example for card payments schemes in 2008 and afterwards for payments instruments, like SEPA direct debit and SEPA credit transfer. Then, our oversight standards for retail payment instruments looked into various areas of risk management such as the financial risks information provided by the actors of the instrument. We looked into aspects of security of the retail payment instruments, operational ability and business continuity. We provided some recommendations concerning the governance arrangements for the different retail payment instruments, as well as about the management for financial risks regarding clearing and settlement, which is behind all these instruments and schemes. We also took an oversight approach to ensure a level playing field was maintained for all the retail payment systems. We developed assessment guides, and these guides were used by the central banks as the driving tool to ensure this.

Currently, we are implementing some regulations to ensure that the previously non-legally binding recommendations are now legally binding. That means that card payment schemes and providers of the retail payment instruments will do what we identified in some of the areas. This is where we actually have implemented the Bank for International Settlements' Principles for Financial Market Infrastructures (PFMI). This is an ECB regulation now, applicable to all systemically important payment systems. Some regulations are applicable to retail payment systems, and some are also applicable to less prominent retail payment systems. Because of this, we also have started a number of assessments. We are at the end of the grace period for large value payment systems and soon the retail payment systems will deliver to us the self-assessments against the standards. Additionally, we have a number of assessments in process concerning oversight of payment schemes, especially on cards where we want to emphasize evidence of the security of Internet payments and on the European direct debit scheme, which has been active for two years.

Concerning retail payment instruments, the European Commission is revising the Payment Services Directive, which aims to introduce regulation for new types of payment services, such as payment initiation and account information services offered by third-party providers. We realized that some new entrants in these markets are afraid that this new regulation will be regarded as a warning, but we believe that the sooner new entrants become regulated, the sooner we can assure they are participating fairly in the payment industry and providing these tools efficiently.

When we saw some cases where the market did not provide what we were expecting, we stepped in as central banks and developed our own retail payment systems. This was the case for some jurisdictions in the euro area where they provided the retail payment systems and we have developed expectations further by also making them systemically important.

Another area where we very actively work is in promoting cooperation between the various sectors. The cooperation is done first among the various national authorities. As you know, we have different authorities in the EU; banking supervisors, securities regulators, and different authorities, so we want to ensure that they all are actively involved. For that reason, we have a number of Eurosystem and ECB related committees. And all these committees work together to define the right standards and principles. For example, we were actively involved in the creation of the SecuRe Pay Forum. This forum brings together overseers from central banks, supervisors, regulators and other euro authorities, plus law enforcement agencies active in the euro area. We discuss and focus on payment security.

In addition, we recently established the European Retail Payments Board. There are many participants from the private sector and various EU authorities. The main focus is to foster standardization and market integration in the EU. Of course, the more choices we have the more responsibility, creating more expectations for the market. For that reason, we want to ensure that what we have developed has been accurately implemented by the central banks and that we have done what has been mandated to us as overseers of these infrastructures.

Further, we have cooperation between the Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO), which are very important in terms of developing standards and new policies for cybersecurity and cyberresilience. We

are awaiting the outcome of the CPMI-IOSCO's work and in the interim are working on a number of initiatives concerning retail payments. So, we are working with various authorities to establish a reporting collaboration scheme for sharing major incidents and information about threats. We also have established forums and task forces for discussing how to improve secure communication and certification, and third-party access to payments accounts. This also will be covered by the Revised Payment Systems Directive. Because there are different regulations and standards, we would like to ensure that all the standards are harmonized among the different regulators in the euro area, and if possible, globally.

In that field, we also would like to ensure that we will establish a new incident reporting scheme, which will have to be done in cooperation with other European authorities, like the banking supervisors. This will be very interesting, once we develop the technology we agree on with them. And yesterday, you heard about our work on fraud management and fraud reports, and we have been actively involved in that field as well.

Finally, we are constantly analyzing various developments. We are in close collaboration with the different market stakeholders. We organize regular conferences on the extent of use with all the different actors in the European landscape. For that reason, we do our analysis before we make our recommendations to our governing bodies.

Mr. Werkema: Thank you. Do any clarifying questions come immediately to mind? We will move to our next presenter, Coen Voormeulen.

Mr. Voormeulen: Good morning, everybody. We have talked a lot about retail fraud, tokenization and passwords. It is very interesting, but I would like to shift the focus. What if the big players—Visa, MasterCard, Fedwire—were attacked by cybercriminals, maybe not to steal money but to destabilize the system. That is a different ballgame. That may even hurt the confidence in the whole financial system, and thus have systemic consequences. That is the same as if the wholesale market would be hurt. Jonathan Williams asked what will be the next step if the payments chain is fully secure. Maybe the wholesale market will be the next target. Then there will be systemic consequences, and that is a big concern for me as an overseer. Therefore, the financial market infrastructures (FMI) are the focus of the group that I am chairing, the Working Group on the Cyber Resilience of CPMI and IOSCO. Those are two international committees for central banks and for market supervisors dealing with standards of the payments

and security sector. It is set up with about 20 countries. What we try to do is to publish guidance notes, one of which is planned to be published for public consultation this November. This guidance note is one step deeper than the existing principles for financial market infrastructures, the PFMI, which was published in 2012, and is the bible for overseers on how to look at FMIs in terms of business continuity, operational risk, legal risk, business risks, (everything ... risk management in general).

In that document, which took a long time to publish, not that much is said about cyber. Therefore, this Working Group on Cyber Resilience was created to go one step further and to see what we can do there. I can talk for hours about that guidance note, but instead I will highlight a few points I consider important.

First, I would say cyber goes much further than information technology (IT). A lot of the discussion in the last one and a half days has been about IT. But when we look at financial market infrastructures, there are several things that maybe are more important than IT. For instance: people. As we know, many attacks on institutions start with social engineering, where people click on malware in an email, in an attachment in an email, and then when the hacker is in, it can go into that organization's critical systems. It is very important that the people in an organization have a clear picture of what they need to do to protect the organization against cybercriminals. So, cyber is also involved in such things like culture. What are you going to do if somebody did something on the Internet of which he thinks, "Oh, that was a mistake." Are you going to punish him? He probably will not mention it then. It is very important to have a culture where people will be open to saying, "Oh, something has gone wrong; I will say it to those who can maybe solve it." It is in line with the saying, "When you see something, say something." When you see that you have made a mistake, say it. But it is not so easy.

Another element is processes. If an institution wants to launch a new product, service or tool, traditionally we like to ask whether it delivers the service; does it do it effectively; is it at low cost; is it speedy enough, user-friendly enough? But we do not always ask the question, if we introduce this new service, what about the whole cyberresiliency profile of my institution? Does it add or diminish risks? That is also important to consider when new services, products or tools are launched.

Finally, an element I think is necessary to stress is communication or collaboration, especially if you look at FMIs. It is actually relevant for every institution. You are never on your own. You are part of an ecosystem that is specifically relevant for FMIs where payments transactions or securities transactions go through many players. So, it is important to communicate with those players not just when there is a crisis. Also, not just to exchange information in advance, what the Financial Services Information Sharing and Analysis Center (FS-ISAC) does, but also, maybe if an institution will be attacked in terms of its integrity. So, if the systems will be corrupted and you need, for instance, to resume after such an attack, you need clean information to restart. Where do you get that clean information? Maybe from your customers, or from third parties, or critical service providers. It is good to have arrangements with those parties in advance, so that after an attack, you can resume quickly.

What about top management? Unfortunately, we also discovered that while top management has a very important role in making sure that their institution's cyberresiliency is at high standards, most in top management are not digital natives. They have gray hair like me, and they consider cyberissues difficult to grasp. It is not their cup of tea. The inclination is to leave it to the IT department. That is not a good choice because the IT department is technically focused, and we need to think about more than that. So, the role of top management to steer a proper cyberresiliency policy needs to be stressed. Unfortunately, it is not always as we would like to see it.

My last point is about what we see now as the biggest risk. I would say that it is the recovery from a successful integrity attack. If an FMI is successfully attacked, and its systems are corrupted, the data are corrupted, a plus is a minus, or three or six zeroes would be behind every transaction. That is really a headache scenario, and what we see is that FMIs in many cases have put a lot of effort in preventive mechanisms; also in the detection of possible cyberattacks, but still a bit less in what to do afterward, how to resume your operations in a safe way. If you just resume, but you have the same vulnerability as before, that is not the best world. You have to resume in a safe way. We clearly see that more attention to that would be very useful, especially because in these PFMI, there is one requirement that says that after an incident—and not specifically mentioned as cyber, but it is also relevant for cyber—you should be back in operation in two hours. There is a two-hour recovery time objective. When we talk to FMIs

about that, they say, “Wow, that is not possible with an integrity attack. It may take even much more than two hours to analyze what is the problem, let alone to get back into operation.” I understand that, but that is thinking in the old framework because these kinds of attacks can happen, and we cannot afford systemically relevant FMIs to take two days to get back into business because in the meantime the financial system might already have been broken down. If you say, “Well, that is too complex to make sure that I am back in business in two hours,” then I think it is necessary to widen the perspective.

Nowadays, many FMIs have a hot standby, and maybe even two hot standbys, in remote locations. That is very useful for many circumstances, but it is not useful if you have an integrity attack, because then you freely copy the malware to your hot standby. That is convenient for the attacker. One possible solution is to have a different standby. It does not have to be in a different location, but in terms of different software, different hardware, maybe different people who made it. In the aviation industry, that is sometimes how they increase security in planes. This might be a solution by thinking in a different framework. FMIs say, “Oh, but that is too expensive.” I think it is not, actually. There are central banks who have this because you can do it in a way that may not be a 100-percent copy of your primary system, but in a way that at least the critical transactions can flow further and maybe in a slightly degraded way, but at least in such a way that the financial system does not collapse.

Again, as I said, we planned to have this guidance note ready for publication in November. We have a two-month public consultation period, so the whole world is invited to react and we are curious what reactions will come. If this guidance note is then published in spring next year, then it is up to individual jurisdictions to lead that into domestic legislation if they want. Then, I think we as a cyberresiliency group are a very small piece of making the world slightly safer.

Mr. Werkema: Thank you. You have shared about systemically important infrastructures and a little about the process you went through. Maybe you could elaborate on that. But then also give us some indication of where there are parallels for retail payments. Obviously, we have talked a lot about retail payments over the last day or so.

Mr. Voormeulen: Yes. The PFMI; they have a clearly defined audience that includes systemically relevant payments systems. We do not want to

change that audience, but I would say we invite countries to apply the same, but in a risk-based manner, to other financial market infrastructures such as not so systemically relevant retail payments. Maybe you can be a bit more relaxed there. But the principles themselves are similarly relevant, and maybe you can, as I said, be slightly more relaxed about how strongly you would implement all the principles. But I would definitely recommend making the retail systems as resilient as possible in this way.

Mr. Werkema: Is there agreement at this point in your group on these six principles?

Mr. Voormeulen: These are just my reflections. The paper is set up a bit differently. It partly follows the National Institute of Standards and Technology (NIST) system to connect it to what is already well-known in the market, and we stress certain things around it. But it is my reflection; I do not think there will be a lot of disagreement in the group.

Mr. Werkema: Good, thank you very much. We will turn to our third panelist now. Anjan.

Mr. Mukherjee: Thanks for the opportunity to address you all today. At the Treasury Department, we are very focused in areas of the “greatest risk.” Obviously, we are all sitting here today because our payments systems nationally and internationally handle staggering sums of money. Just in the Federal Reserve System through the 12 banks, there is something like \$4 trillion per day that goes through the system, which is a quarter of annual GDP in the United States. And the total volume of payment activity annually is approaching \$200 trillion, which is a staggering sum. So, we tend to go where the big dollars are in terms of risk focus. We note that much of the architecture that underlies the payment systems, that supports this massive volume of activity, is legacy in nature and subject to the rapid technological change that we see today—the rise in mobile computing, the greater ubiquity of high speed networks, ever accelerating transaction processing speeds. And so the combination of the legacy systems with a time of rapid technological change not only means that it is an exciting time in the world of payments in that some of these innovations may fundamentally change the architecture of the payments systems as we look to the future, but it also means that there is a need to be extraordinarily cautious. When you have this sort of combination come together, the underbelly of the rapid acceleration is the ever-increasing technological threats as well. The payments system, as I think of it, was initially built for connectivity, not for

security. So, we pay real attention to cybersecurity threats. It is an issue of real importance to us at Treasury, obviously the nation as a whole. Part of what I do is oversee the Office of Critical Infrastructure Protection, which among other things has the responsibility for monitoring and facilitating the protection of critical infrastructure in the nation's financial services industry, which includes our wholesale payments systems. We want to also ensure that the retail payments systems have the level of security needed to protect the work efficiently and protect consumers' private information.

We remain vigilant because it does not take much to imagine an attack on a wholesale system that could be crippling, as Coen says, and affect consumer confidence. And on the retail side, we are already well aware of some of the breach activity that has led to divulging private information, which we are trying to prevent. In our role as Treasury and sort of an organizer in the executive branch around the financial sector, we operate on multiple levels. We try to coordinate and facilitate administrative executive level activity as well as legislation on the former to address some of these issues. You may have seen recent executive orders that the president has issued on some of these issues. One thing we did in October, was an executive order around retail payments, accelerating the security of retail payments where we as a government felt that we had almost a priming-the-pump type function when it comes to retail security. We announced our Buy Secure Initiative, which is an initiative to roll out EMV chip and PIN technology in the existing and future government card network, and also to replace all the retail terminals in the government system to make them compatible with EMV as a way to harness the government's purchasing power. You have recently seen a sanctions executive order that is targeted at malicious cyberactors where the Treasury Department will use its sanctions authority to specifically deter cyberattacks. And then at the beginning of the year, we helped formulate and coordinate the administration's legislative proposals on cybersecurity, which looked to facilitate information sharing and data breach notification and a few other things that we can talk a little more about.

So having set that stage, I want to focus these opening comments on a few areas where I think government and the private sector can work effectively together to promote a more reliable, secure and resilient payment system, both on the wholesale and retail sides. In fact, in some ways at Treasury our entire framework for dealing with cybersecurity issues roughly falls into the following categories. First, it is promoting best practices and baseline

protections; second, is sharing threat information; and third is improving response and recovery planning. We have heard about elements of each of those throughout the conference and earlier this morning, but I wanted to talk about them in more detail.

First, on best practices: These are the policies, procedures and other controls that an organization will adopt to prevent penetration of their networks by malicious actors. As Coen just mentioned, the NIST framework for improving critical infrastructure cybersecurity is one of the best examples of a set of practices. The core five functions are identify, protect, detect, respond and recover. This is a tool to help systematize your organizational cybersecurity. If you are not using NIST framework, you should be. Probably everyone in this room is well familiar with it. NIST is working on evolving the framework, but I would encourage you all to do the same. It is really a foundational starting point to think about, not only the narrow issue of cybersecurity risk, but really the broader issue of risk management and organizational resiliency. So I hope you build upon this framework to more deeply embed organizational risk management into your business strategy.

As for baseline protections, there is a lot of interesting technology that is evolving. We have heard about some of that over the course of this conference. I would simply encourage everyone to examine moving toward more state-of-the-art security solutions; advancements one ought to embrace. Whether it is around encryption and authentication solutions, making sure everyone is completely compliant with ISO 20022 standards, moving to more of a credit push as opposed to a debit pull model as we think about money transfer, we think there are some important technological advancements. We do not endorse any one of them, but we encourage you all to explore them more carefully and embrace the ones that make sense for your organizations.

Next, I would like to highlight the importance of information sharing in this arena. I think this is one of our most potent tools to counter malicious cyberactivity. To reduce risk over time, we have to understand the threats we face. Many times the best way to do this is by looking at other entities and sharing information—the threats that someone else faces, that your organization faces, other entities could benefit from learning about. The malicious cyberactors are sharing information and tools all the time. We on the government side and the public and private sectors together should be doing the same thing, obviously in a way that protects privacy and business reputation.

As I mentioned, in January the president sent an information-sharing legislative proposal to Congress that included things like liability protections to encourage companies to share cyberthreat information, and to encourage industries to set up information sharing and analysis organizations (ISAOs), and we are firmly behind that. I hope we can talk some today about the extent to which major payments system stakeholders are engaged in such information sharing, including through our friends at the FS-ISAC that we heard from this morning.

The last area I want to address relates to response and recovery. Obviously, there is no such thing as complete security. So we really have to do everything we can to prevent the initial attack, but also to be prepared when an attack occurs. It is important for us to maintain both national and organizational incident response plans that make your incident response process much more effective, predictable and efficient. We encourage all organizations we deal with to have very strong incident response plans in place, and to exercise them. Exercising these plans really helps senior management, the security teams, external stakeholders, all the various constituents to be comfortable with their particular roles and responsibilities when and if an attack occurs. So I would just ask a few questions around this: When was the last time you exercised your incident response plan? How were your third-party service providers pulled into this effort, because we think that is very important when thinking about this question. How did you include your external stakeholders, such as law enforcement or your regulator, if that is appropriate, or Treasury? These are just some questions to consider.

I will close by emphasizing that this cybersecurity issue is really all about collaboration—public and private collaboration. There is no single government agency that has sole responsibility over this issue. So we collaborate within the government, and it is critically important. This is an issue that is cross-cutting, so it is incumbent upon us to collaborate among the private and the public sectors. Adopting these baseline protections and best practices, sharing threat information, improving our response and recovery posture is critical. All of it will benefit from collaboration between public and private, and ultimately that is to the benefit of protecting the integrity of our payments systems, which nationally and internationally are a real resource.

Mr. Werkema: Thank you, Anjan. Any clarifying questions? OK, perhaps I will give a question about financial market infrastructure to all three of you. Obviously, the countries represented are key players. Talk about

communication and coordination between key financial market infrastructures on these issues of resiliency and cybersecurity.

Mr. Tsiliberdis: In Europe we are organizing a crisis communication test where we have invited the major payments infrastructures and a number of banks to participate. Our objective is to test the crisis communications arrangements and also how they will react in such a cybersecurity event. We place a lot of emphasis on this. For that reason, we have established a specialized task force to implement this procedure and this exercise. Until now, we have realized that in the euro area, we had mainly conducted exercises organized by the systems, but nothing was done in terms of marketwide exercises. So this is one of the first steps that we are doing in this area.

We also are promoting information sharing between the different FMIs. That is why as I mentioned there is a new specific process between the SecuRe Pay Forum and other forums where we try to bring together the different regulators and law enforcement agencies to exchange information about cybersecurity threats and other risks or incidents, which are occurring on a daily basis in our infrastructures.

Mr. Voormeulen: The interesting thing in the Working Group on Cyber Resilience is that the optimal way of coordination is very different from country to country not just because of different legal setups, but also different historical and cultural habits. There are countries where the regulator needs to push cooperation. Otherwise, it does not come across. There are also countries where if the regulator steps in, then the coordination stops. The markets themselves do that much better. But I would say that in any case, it is important within your own cultural environment to stimulate coordination by many different things. The CERTs were mentioned several times. That is on a very practical level. The FS-ISAC was mentioned. You also can do crisis management exercises nationwide. That is what we do in the Netherlands. For the last three years, these crisis management exercises always have been about cyber, and not about any physical accident. We are now trying to expand that. So far, it is in the financial sector, so all players are there. But we are trying now to expand it to the energy and telecommunications sectors because those are crucial players also for the financial sectors. Without telecommunication, we cannot do a lot anymore. So we have our own, we call it FI-ISAC, but essentially it is the same thing. But for me, the biggest struggle is how to get it off the ground internationally because the borders are not relevant for attackers. So in the end, it is all

about international issues. But it is very difficult to set up an international forum for official collaboration. This Working Group is a little tiny effort to do that. But maybe an option is what we heard this morning, the FS-ISAC is expanding internationally because the institutions that are involved are international institutions. They have business in other countries as well. So maybe that is also a good way to make a step forward.

Mr. Mukherjee: Yes. I was going to underscore what Coen said at the very end, which is that challenges are around international coordination. When we look at FMIs, even within a single FMI, there are barriers to information sharing due to security clearances or confidentiality agreements. That is within the FMI entity. Now if it is a global FMI, you have the home authority, you have the host authority, and these sometimes are conflicting and I am not sure we have done enough yet to coordinate across border. So we support the work at CPMI-IOSCO around this and we have input there. I think that is where we will start the lead. I will say that we are starting to create exercises. We are very supportive of the crisis management group efforts and the exercise that Coen mentions, that is often done on a national level. I think the next step for us is to try to tackle that on an international level and deal with the cross-border issues. But we will get there. We are establishing not on FMI specifically, but more broadly, an exercise that the United States will do with the U.K. either later this year or early next year. I view that as a first step toward more of an international exercising regime that we can utilize to test these questions around FMIs in particular.