

# Conference Summary



*Terri Bradford*

## **I. Introduction**

Cyberattacks and large-scale data breaches that expose the sensitive information of millions of consumers and result in billions of dollars of fraudulent payment transactions have elevated payments security to a forefront issue. In 2014 there were 783 data breaches in the United States that exposed more than 85 million records.<sup>1</sup> Although U.S. retail payment systems do not receive the same scrutiny as large-value payment systems, the public expects them to work without fail every day; their smooth functioning is critical to the public's confidence in new and more efficient ways to pay. As a consequence, payment participants—end users who make payments, financial institutions and nonbanks that provide payment services, and networks and service providers that process payments—all have considerable incentive to secure payments and deter fraud.

As industry participants look for ways to improve payments security, there are many issues with which to contend. Among them are key policy questions such as: What economic principles underlie the determinants of payments security? What options are available to better align incentives of payments stakeholders? How best are resources allocated between preventing, detecting and responding to payments security threats? How should the changing threat landscape affect the ways in which sensitive information is secured and used for retail payments? What are the roles of private players and public authorities, given coordination problems and challenges in obtaining data on payments fraud and other security indicators?

These and other key policy questions create a puzzle for the myriad of payments participants to solve, and formed the motivation for the Federal Reserve Bank of Kansas City's fifth international policy conference titled, "The Puzzle of Payments Security: Fitting the Pieces Together to Protect the

Retail Payments System.” The conference was hosted on June 25-26, 2015, in Kansas City, Mo. During six sessions and two keynote addresses, more than 120 payments system participants and observers exchanged thoughts and views on payments security and fraud as matters of importance for preserving public confidence in payment systems around the globe.

Each session focused on one of the motivating policy questions. The following summarizes each session of the conference, highlighting key insights, areas of agreement and points of contention.

## **II. Opening Remarks: An Opportunity to Consider Solutions**

Kelly J. Dubbert, first vice president and chief operating officer of the Federal Reserve Bank of Kansas City, opened the conference by acknowledging the complexity involved in securing the retail payments system. Dubbert noted that while security has never been simple, the issue has become more complex because of the pace of growth and innovation within the payments system and the many participants, technologies and issues involved. The flow of goods and services relies on a well-functioning payments system, and security has always been a key component of those transactions, which are a critical part of the economy. Dubbert added that while central banks have an important role in assuring public confidence in the system, more broadly, payments security requires the active engagement of the spectrum of payments system participants. As the central bank for the United States, and as both an operator of retail payment systems and an overseer of the financial institutions that many use to access the payments system, the Federal Reserve is in a unique position to promote the involvement of the respective industry segments. Dubbert said the puzzle of payments security we face today cannot be solved by working separately. He urged participants to use the conference as an opportunity to consider how available solutions can be leveraged collectively to address the payment system’s broader challenges.

## **III. Keynote Address: Building a Safer Payments System through Collective Action**

Federal Reserve Gov. Jerome H. Powell provided the conference keynote in which he described the importance of payments participants working together to maintain and enhance a safe and secure payments system. He discussed the Federal Reserve’s current efforts to improve the speed,

efficiency and security of the payments system, pointing to the consultation paper published in 2013 that sought public input on ways to make the U.S. payments system safer, more accessible, faster and more efficient from end-to-end; the release of a second paper in 2015 that outlined strategies for improving the U.S. payments system, and the subsequent establishment of two task forces: one for faster payments and one for payments security.

Powell then stressed that payment system participants must work together by participating in coordinated efforts to improve the payments system. He noted that the market should be the primary driver of change, and government should avoid stifling healthy innovation. During the balance of his remarks he spoke about four actions all payments participants need to take with respect to payments security. The first is to embrace safe innovation, while prudently managing new risks that may be introduced by new technologies. The second is to implement preventative tools—defensive tactics—because it is not a matter of if there will be an attack, but rather when. The third is to complement prevention with a comprehensive payment security plan. And the fourth is to collectively educate consumers to empower them to safely use financial products.

Concluding his remarks, Powell asked for the support of payments system participants in building a safer and more efficient payments system. He noted that a high level of engagement will be critical and encouraged participation in one of the Federal Reserve's task forces and in providing feedback.

During the question and answer period, participants asked Powell about his reaction to the breach at the Office of Personnel Management (OPM), and about the role of the Federal Reserve: should it use its dual roles of operator and regulator to drive which aspects of security are put in place by market players; is there really a universal case favoring faster payments; can it really help the United States catch up to the rest of the world? Powell indicated the Fed was looking closely at the OPM breach, trying to understand what happened and how that information can be used to safeguard the System's employees. He added that while the Fed does have regulatory and supervisory authority over banks, its plenary authority does not extend over the financial system or the whole payments system. As for faster payments, Powell agreed consumers and businesses want faster payments but that not every payment needs to be made instantaneously. Innovation, Powell said, and a more flexible economy will enable the United States to catch up and pass the rest of the world.

#### IV. The Economics of Payments Security

In the opening session, “The Economics of Payments Security,” Tyler Moore of Southern Methodist University presented a paper he co-authored with Fumiko Hayashi and Richard J. Sullivan, both from the Federal Reserve Bank of Kansas City, that discussed how economics can help to better understand the dynamics of retail payments security and explain why the payments system is not moving as quickly as it might to better, more secure technologies. Moore outlined the basic economic principles that characterize retail payments markets; network externalities, two-sided markets and economies of scale and scope, as well as principles that pertain particularly to payments security; jointly produced goods, competition for the market, asymmetric information, moral hazard and trade-offs that occur between information sharing and privacy. After explaining how these principles are related to challenges to effective payments security, Moore discussed how the game theory approach can be used to evaluate and construct strategies that can achieve socially desirable levels of payments security.

To illustrate the value of modeling payments security scenarios using game theory, Moore offered four case studies where incentives appear insufficient to adequately secure payments. The first concerned fraud in card-not-present (CNP) payments, such as online payments where the card is not physically presented to a merchant. The second case study illustrated inadequate protection of sensitive payment data that is useful for committing payment fraud. The third and fourth case studies were mobile payments and cryptocurrencies, both of which are potentially more secure than existing payment methods but also face additional challenges, such as adoption by end users and establishment of control structures that ensure integrity of the overall payments ecosystem. Moore used these case studies to demonstrate that the interdependence in modern payments systems poses significant challenges to improving security, which may make the status quo appear satisfactory.

Moore noted that in each case study, leadership of collaborative efforts is important to appropriately modify games of collaboration, and thus achieve socially desirable levels of payments security. More specifically, leadership should modify games of coordination so that the best-positioned payment participant has enough incentive to balance the incremental costs of security against the incremental reduction in fraud, data breaches and other security incidents. He offered that effective leadership requires strong

commitment, credibility and an understanding of conflicts of interests across various parties. He said these attributes help leaders effectively reconcile the conflicts of interests and build trust among involved parties. That trust then may lead to collaboration on rules or guidelines concerning property rights, distribution of costs and liability, or limited available options to each party. The attributes also help leaders improve involved parties' expectations for prospects and outcomes of collaboration and thereby induce these parties to collaborate effectively.

Moore concluded that the biggest challenges to adopting socially desirable levels of payments security are economic not technical. Competing interests and incentives may inhibit adoption of more secure technologies. As a result, coordination among stakeholders is essential, and game theory can uncover superior outcomes as well as strategies to attain them. Moore noted that public authorities and academics, due to long-term vision and societal outlook, can help overcome barriers to collaboration.

Adam Levitin of the Georgetown University Law Center was Moore's discussant. Levitin agreed that game theory provides a foundation from which the understudied area of payments security economics can begin to be better approached, but that externalities and spillover effects to third parties are not accounted for in the application of the theory. Levitin critiqued the paper's assumptions about knowledge, causation, the bilateral nature of the game and the use of binary choice; however, he acknowledged that the game theory assumptions are valuable in pointing out where to focus payments security policy. Levitin suggested that the policy agenda for payment security should focus on better data collection, better antitrust enforcement and reducing externalities without creating unintended consequences.

Levitin also said private or public ordering—self regulation or government intervention—can be used to achieve the goal of greater payments security in different contexts. He noted that neither is perfect. There are issues with private ordering; and it is less clear how good of a result can be achieved with public ordering. That said, Levitin observed that public ordering is the direction in which payments security policy appears to be gravitating; driven in large part by headlines about data breaches, which are creating legislative and regulatory interest and national security concerns.

Responding first to Levitin's commentary, Moore opened the discussion period by agreeing that game theory does not account for externalities

and that the models ignore them. He added that the real conversation of externalities takes place in the public/social optimum, motivating the need for greater public oversight and involvement. However, because it is doubtful public authorities will come up with better solutions, it is important that the private sector remain engaged. Questions from the audience ranged from whether Bitcoin can be a long-term viable retail payment system to whether zero fraud in the payments system is the correct policy goal. Levitin noted that it is hard to see Bitcoin being attractive in stable economies; but the underlying blockchain technology could be valuable. Moore added there is technical innovation with a distributed secure system that could be available. Levitin and Moore both argued against the concept of zero fraud being attainable, with Levitin favoring getting to a point where the marginal losses due to fraud equal the marginal cost of fraud prevention.

Moore and Levitin concluded that while game theory works well to analyze an idealized version of the world there is not any one correct security setting for all payments, but there are some policy principles that should be pursued. First, data collection in standardized forms is a key to applying game theory to the real world. Second, from a policy perspective, ideal security strategies should be broad in scope and meet longer-term needs rather than achieve a single security improvement. Third, to encourage participation in such strategies, it is important that costs and benefits be fairly distributed among participants.

## **V. Monitoring Payment Fraud: A Key Piece to the Puzzle**

In the session “Monitoring Payment Fraud: A Key Piece to the Puzzle,” Alexandre Stervinou of the Banque de France’s Observatory for Payment Card Security and Chris Hamilton of the Australian Payments Clearing Association (APCA) shared insights from their experiences collecting and analyzing payments data and data facilitating payment security improvements.<sup>2</sup>

Stervinou said the Observatory monitors security measures adopted by issuers and merchants, establishes aggregate fraud statistics and maintains a technology watch for payment cards. The Observatory started collecting data to better understand fraud rates, its prevalence and where it originated and produced its first annual report of fraud data in 2006. Stervinou said that from the information the Observatory has gathered, it has generated fraud statistics, identified trends, made recommendations, and closely monitored security measures deployed by issuers/banks and merchants.

One outcome of the Observatory's data collection efforts has been a push for stronger customer authentication in online transactions. Stervinou said the Observatory strongly advocated use of two-factor authentication and encouraged the use of 3D Secure.<sup>3</sup> The Observatory worked to convince involved parties that there were incentives for adopting these stronger security methods and allowed for a risk-based approach for deploying stronger authentication. The Observatory recognized that for its efforts to be most effective it needed a broader approach, one that was not "French-only." As a result, it supported the emergence of a European forum for supervisors and central bankers through which there was a successful legislative push to require strong two-factor authentication. Stervinou added that the European Banking Authority released guidelines in December 2014 on securing online payments across the European Union (EU), including an implementation deadline of Aug. 1, 2015, for EU companies to begin research and deployment.

Hamilton offered a private-sector perspective, noting that 10 years ago, after concluding the lack of investment in payment security was partly due to the lack of appropriate data, APCA began collecting data to better understand fraud rates and prevalence, the consequence of fraud and the threat matrix. Hamilton said data is essential for risk management capability and for enhancing public debate when arguing for security improvements. With the data, an impact analysis can identify what happens when fraud occurs—who ultimately bears the losses, what are the real costs and the cost of implementing new security technologies. Hamilton said reporting requires cooperation, which has helped participating organizations manage their own fraud. Hamilton noted that APCA has found that, in contrast to the approach taken by the Observatory, data capture and reporting are better done when voluntary than when required by regulation. It is more cost effective and also enables a greater focus on industry needs; however, he conceded that the quality of the data has room to improve. Hamilton added that APCA also shares the information with the public to broaden the awareness of fraud and its prevention.

Stervinou, responding to Hamilton's commentary, said the decision to intervene in security and collect data are two separate things. Banque de France wanted to intervene to improve security, but to determine the appropriate intervention and issue recommendations, he said, the central bank had to have the necessary data. Stervinou added it is important to find

the right balance between regulation and innovation by market players. As a public authority the Banque de France offered neutrality, which is very important because security must not be a competitive issue.

Participants' questions ranged from why the United States is undergoing an expensive conversion to Europay, MasterCard and Visa (EMV) chip payment cards without mandating personal identification numbers (PINs) to whether collecting and publishing fraud data has the unintended consequence of increasing consumers' fear of fraud. Stervinou and Hamilton agreed a better approach in the United States would be chip and PIN; Stervinou added "chip is half the way through; it is a good half, but it is still half the way through." Hamilton said the annual reports Australia releases on fraud have actually reduced consumers' fears about fraud. Stervinou added that the release of fraud statistics is a good opportunity to remind consumers of their responsibility to help safeguard their information.

Stervinou and Hamilton agreed that data collection is essential to understanding rates, the prevalence and origination of fraud, and facilitates an understanding of the real costs of fraud and security breaches. Hamilton said ultimately, what can be measured can be managed and attempting to choose between private action and public intervention is likely a false dichotomy. Stervinou added the private and public sectors need to work in tandem because fraud and payments security are everyone's concern. They concurred that a collaborative approach to collecting data on fraud and payments security incidents is most beneficial. Ultimately, facts will make for better public debate about how best to allocate resources.

## **VI. Luncheon Keynote: Achieving a Resilient Cyber Ecosystem: A Way Ahead**

Peter Fonash of the U.S. Department of Homeland Security (DHS) spoke about the cyber ecosystem and the efforts under way at DHS to raise the level of cybersecurity for the whole country. Fonash explained because cybersecurity is everyone's concern, raising the overall security of the ecosystem is needed. He provided evidence that 10 years ago adversaries were more effective in attacking the cyber ecosystem than the industry in detecting intrusions and the gap has grown. He said the Internet of Things will drive enormous growth in the scale and scope of potential cybersecurity intrusions; expanding devices accessible via the Internet—including cars, refrigerators, home heating systems—that are not actually under anyone's security control

will make it difficult to effectively provide security for controlled enterprises. Moreover, he observed organizations' budgets today are mostly flat or decreasing and staffing levels are insufficient to address the problem.

Fonash said the effectiveness of cybersecurity needs to be improved. The security analysts today have incomplete knowledge of their individual organizations and what is happening in the Internet in general, but they need to become more productive. The time to detect and respond to a cybersecurity intrusion needs to be reduced from months to days or minutes. Although there are a lot of innovations in the research community, better management of the process of inserting innovations into existing systems is needed. There needs to be a move away from the model of treating all data as equal to a risk-based framework.

Fonash said these improvements can be accomplished with industry consensus on interoperability, automation, trust and information sharing. He defined interoperability as the integration of tools into a tool set with common semantics and syntax of data so as to provide security analysts with a common understanding of what the data mean without spending too much time reconciling data that only appear to be different. Interoperability enables automated courses of action; sensing an intrusion, making sense of that intrusion, making a decision on how to block it and taking action to implement that decision. While Fonash acknowledged concerns in terms of unintended consequences of the automation, he noted those concerns could be overcome through a better understanding of automation and its consequences and implementing mechanisms to allow for a quick reversal of automated actions. Trust among participants in the cyber ecosystem is critical for information sharing. To build trust, Fonash said, partnerships with the Information Sharing and Analysis Centers (ISACs), and now Information Sharing and Analysis Organizations (ISAOs), are facilitating the organized sharing of best practices. Another critical piece for information sharing is an infrastructure that supports resilient communications. Fonash noted the infrastructure is currently transitioning from a circuit-switch technology to an IP-based technology. Also, DHS uses a motto of "see something, say something" to facilitate information sharing; if you see something with regard to cybersecurity, report it to the rest of the ecosystem so action can be taken to patch the vulnerability and potentially avoid attack. Fonash said the government will facilitate these ideas and actions, but the desire is to have industry lead.

Discussion during the question and answer period focused on financial and nonfinancial incentives that might motivate the private sector to innovate and collaborate, the international component of what DHS is doing to help foster standards and how to mitigate some of the risk across multiple industries related to the growth of the Internet of Things. Fonash pointed out part of the problem in any discussion about security is the threat is always changing and that fraudsters are better and quicker right now than the industry—a cottage security industry versus an automated adversary. He suggested that government will influence adoption by bearing the cost of developing and setting specifications and then making them part of the contracting process for both DHS and the Department of Defense. Data standards, he said, are a necessary component of working with other countries, adding that the United States does partner with other countries in these efforts. Fonash said it would be more desirable to have security built in to devices rather than added on to mitigate risks, adding he can see Internet service providers offering services covering all of a consumer's devices, such as smart refrigerators and dishwashers.

## **VII. Managing the Threats to Data Security**

The session “Managing the Threats to Data Security” addressed how—even with various security standards, protocols and procedures in place—breaches and vulnerabilities have progressed. During a panel moderated by Tracy Kitten of Information Security Group, Mark Carney of FireMon, Robert Carr of Heartland Payments Systems, Liz Garner of the Merchant Advisory Group and Vernon Marshall of American Express discussed what the payments industry needs to do to enhance data security and why it is not already taking more action.

Among the standards discussed were the Payment Card Industry Data Security Standards (PCI DSS). The panel agreed that though there is a need for a risk-based, consultative approach to compliance with these standards, the natural tendency is a check-list mentality. So, instead of being gray, the assessment process is black and white. Carr observed that PCI compliance is assessed at a moment in time; however, if a breach occurs, the implication is that the merchant or processor was no longer in compliance. Carney noted that entities have different challenges with compliance. For large merchants, it is about scope and/or scale, while for smaller merchants the problem is lack of knowledge and resources to respond. Carney added

that the range of emerging payments technologies has security implications that should be considered, and that present challenges for the standards body to keep up with. Garner advocated for open standards to help promote incentives to comply with PCI. Panelists suggested that without a centralized platform to protect against breaches, compliance with PCI DSS is a confusing process at best.

The conversation then shifted from requirements designed to ensure secure processing, storage and transmission of payments data within and across organizations to the U.S. migration to EMV chip and signature standards, which target securing the point of sale (POS). Carr discussed the investment his company made years ago to develop a POS encryption technology that enables encryption that protects card data from the point of capture throughout the transaction to the point at which the data are decrypted. He asserted that even if stolen, criminals cannot use the encrypted data to create counterfeit cards or make fraudulent CNP transactions, as long as the keys to decrypt the data are not stolen. Garner cited statistics suggesting that merchants bear 38 percent of fraud, issuers bear 60 percent and consumers bear 2 percent; however, absent from that equation are the networks that developed the EMV technology, who bear no cost if the technology fails to become adopted or provides inadequate security. Further, the majority of the panel indicated the most secure option would include PIN authentication instead of signature and questioned why networks are not promoting that option. Marshall said PIN presently is not widely deployed at merchant locations. He said there was a desire to ensure the most consistent customer experience. Customer service is paramount and security is an aspect of customer experience. So, the decision was made to deploy chip and signature, which provides roughly 80 percent of the benefit. However, Marshall noted that preparations are under way at American Express for chip and PIN.

From the POS, the conversation shifted to discussion about CNP transactions, for which fraud is anticipated to increase as a result of the migration to EMV. CNP fraud is costly and, according to Garner, merchants bear 74 percent of that fraud. Garner said in the online environment, the lack of multifactor authentication on payment cards is the culprit. For merchants, it is a difficult investment decision, and for issuers, there is a possibility they may lose top-of-wallet status. Still, doing the right thing for security suggests the need for multifactor authentication.

Questions about the role of the Federal Reserve generated some lively discussion among panelists and participants. Marshall noted one obvious contribution the Fed could make would be to do the same type of fraud-loss reporting as in France and the United Kingdom. Kitten observed that discussions in years past made it clear the Fed did not want a hands-on role in overseeing the migration to EMV and that it should fall to the private sector. Garner praised the efforts of the Fed's current task force to bring stakeholders together to discuss a number of security issues.<sup>4</sup> Carr added that having the Fed, as the most respected institution in the ecosystem, recommend best practices would be better than what is in place now. Another question centered on the fact that although the industry has spent billions on fraud prevention, fraudsters are still out-innovating the industry; asking is it time to forget about protecting the system and figure out how to do clean transactions in a dirty system? Marshall suggested solving the problem by first protecting the data and also protecting usage. Carr referred to a remark from Powell's keynote, that "Preventative measures are not adequate" and do nothing to guard against a host of potential threats from within—employees. As the panel concluded, there was agreement that while each deployment of enhanced security standards chips away at the larger issue, no one security standard or application is the "silver bullet." Instead, a multipronged security approach—EMV, encryption and tokenization—is needed.

### **VIII. Devaluing Data: If the System Cannot Be Made Secure, Can the Information Be Made Worthless?**

The session "Devaluing Data: If the System Cannot Be Made Secure, Can the Information Be Made Worthless?" built upon sentiments shared in the previous session, examining ways in which payments data can be devalued. During a panel moderated by Marianne Crowe of the Federal Reserve Bank of Boston, panelists representing network, issuer, processor and standards committee perspectives discussed how tools such as tokenization and end-to-end encryption can be used to enhance payments security.

As the dialog began, Steve Schmalz of RSA, The Security Division of EMC, urged that a first order of business was clarification of what "tokenization" entails and suggested that the notion of it as a "magic door" needs to be dispelled. He noted there are pre-authorization tokens, which can be used to initiate the transaction, and post-authorization tokens that act as

a pointer that allows for retrieval of the primary account number (PAN) when it is needed. Each type of token has a different risk profile.

Radha Suvarna of Citibank remarked that EMV, tokenization and point-to-point encryption together provide an opportunity to drive better value and enhance the security of the payment ecosystem. None of these by itself is the silver bullet. But together, they begin to deliver a better, more secure solution for consumers by making the transaction information less useful. Suvarna said tokenization allows the context in which the payment is being used to become a determining factor in whether to accept or decline a transaction. Madu Vasu of Visa shared how tokens for mobile payments, such as those offered by Apple and Google, are created and provisioned onto a mobile application. Both Suvarna and Vasu agreed that tokenization coupled with EMV cards makes payment transactions more secure by devaluing the underlying data. So even if the token is compromised and used in a CNP transaction, it would not get authorized.

Branden Williams of First Data Corp. noted that tokenization has turned into this year's version of big data, the cloud or virtualization, where people do not necessarily know what it means or, perhaps more importantly, what it means to them. He said that aside from trying to reduce PCI scope by deploying technologies like tokenization, the industry is marching along to the beat of the PCI drum, and nobody has stopped to ask why, whether it really makes sense, or if the problems that we need to be solving are actually being solved.

On the matter of encryption, Schmalz suggested use of the term “cryptographic mechanism” because a lot can be done with cryptography other than just encrypting something; for example, a digital signature can be created. Schmalz noted that a digital signature enables not only confidentiality, but also protects the value of a transaction and its integrity. Further, it facilitates repudiation, and ensures that information cannot be changed; in essence it locks information in so a certain piece of the information can only be used in a certain way. Vasu added that a hybrid solution based on needs is very important. As an example she noted a combination of encryption with tokenization with the payment account reference (PAR) is important for merchants.<sup>5</sup> The PAR basically gives the ability to tie the payment credential across multiple token requesters.

The discussion progressed to security issues associated with storing

tokens. Vasu offered that from a network perspective, the pre-authorization token is protected in a highly secure zone and the provider is the only one who has the ability to detokenize. Schmalz noted the ANSI ASC X9 F6 tokenization standard addresses how to secure what is called the tokenization service, which includes that vault, and addresses how to secure authentication and authorization, the ability to ask for a token or detokenization services, etc.<sup>6</sup>

With mobile, provisioning of the pre-authorization token depends on the provider: secure element on the device or host card emulation (HCE) in the cloud. Vasu acknowledged there are some security concerns with HCE; but those have been addressed with a limited use key that is dynamic in nature, and has certain parameters or thresholds like the number of transactions, the transaction amount and the usage. Suvarna added that there is a need for a ubiquitous solution that drives consistency and provides volume, but regardless of whether secure element or HCE, mobile transactions made with a token are more secure than those without.

For CNP and e-commerce transactions, panelists agreed that pre-authorization tokens are applicable. B. Williams observed that tokens whose standards were developed by EMVCo are utilized by Apple Pay and there is an opportunity for companies that have mobile apps to follow suit. However, he also noted that whether tokens actually solve the CNP problem warrants examination. Suvarna stressed that while tokenization is a great technology, mobile apps, at best, only represent 0.01 percent of payments volume and that tokenization needs to be applied where the volumes are; where the ecosystem can more fully realize the benefits.

During the audience question and answer period, a question was posed about what can be done to devalue a card number and its use on a computer that might have malware, and also on the merchant back-end networks. Panelists generally agreed there is little to be done to protect a consumer from using a computer that has malware. Schmalz suggested it might be possible to produce a token that detects endpoints that have malware on them and then alert the owner and/or reject transaction, but there still would have to be some form of intervention. Vasu noted there have been discussions with companies in the browser business about using tokenization but that has been described as a huge effort. B. Williams agreed the industry cannot protect the consumer who has malware, adding consumers have to participate in their own rescue.

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

In the session “Role of Industry Collaboration in Payments System Security,” industry executives—within and across sectors of the payments system—addressed how they are making a joint commitment to advance payments security through dedicating time and resources to plan, advance recommendations, communicate and educate. Moderator Jonathan Williams of Experian set the scene, saying societal good is the real driver of many of the collaborative efforts under way. There is a need to share intelligence and develop common standards and systems to protect not just individual institutions but the whole payments system, including customers. J. Williams noted there are different types of collaboration, questions about on what to collaborate and when to engage. Throughout, there is a focus on what we are trying to protect. J. Williams said the various collaborative efforts represented by the panelists offered insight into leading practices.

Charles Bretz of the Financial Services-ISAC (FS-ISAC) shared that his organization was formed by the financial services industry to protect the sector from cyberattacks. FS-ISAC processes thousands of threat indicators a month—sometimes thousands a day—and has grown rapidly with 5,900 participating institutions, about 2,500 of which are financial institutions bound by its operating rules, nondisclosure agreements and under contract to share information. Bretz noted that in recognition that threats extend beyond U.S. borders, FS-ISAC has expanded to include members in Western Europe, Australia, Singapore and Japan. Membership in South America also is anticipated.

Representing the Payments Security Task Force (PSTF), Nancy O’Malley spoke about work to secure card-present transactions. The PSTF is an initiative launched by MasterCard in response to concern about the progress being made toward the migration of EMV in the U.S. marketplace. The PSTF was convened to foster a different level of collaboration at the most senior level of the payments security marketplace with the goal of gaining and securing commitment to advancing solutions purely in the safety and security space.

Sandra Kennedy of the Merchant Financial Services Cybersecurity Partnership shared the organization was formed out of a need for retailers to collaborate on a plan to address security incidents. As a first step, the Retail

Industry Leaders Association (RILA) reached out to the Financial Services Roundtable (FSR). Kennedy noted that after finding common ground on many issues, the groups decided to focus on those and move forward collectively. RILA and FSR pulled together 19 associations representing the merchant and financial services industries to focus on five key areas. Through this partnership, RILA learned much from the financial institutions involved as well as FS-ISAC and other organizations. Kennedy said that with the assistance, knowledge and experiences of these other associations, RILA was able to establish a Retail Cyber Intelligence Sharing Center, which will house the retail ISAC. She noted that, now almost a year old, the sharing center has forged a formal relationship with the FS-ISAC that will be a long-term benefit to both sectors.

Liz Votaw of the Fast IDentity Online (FIDO) Alliance observed that the FIDO Alliance is a little bit different from some of the other collaborations, but there also are similarities. What makes FIDO different is that it is not a payment-specific collaboration. It is a cross section of every type of company involved in authentication; its focus is on helping companies throughout the authentication ecosystem ensure that their implementations of authentication technology are safe and secure not only for the companies but also for their customers. Votaw said the Alliance has led to the development of a set of specifications that industries can leverage to rid themselves of reliance on passwords for authentication.

J. Williams asked how the effectiveness of these collaborations can be measured. Panelists agreed that it varies. Bretz offered that objectively, there are many metrics and the more statistics that can be collected the better. However, metrics present a challenge in that reliable statistics are rare. O'Malley and Kennedy suggested that success also can be measured subjectively, by sustained commitment to partnerships and networks that are built, which historically has not been the norm in the payments ecosystem. Votaw added that adoption of practices and specifications offers another objective measure of success.

As for challenges to collaborations, O'Malley identified overlapping initiatives of many well-intentioned groups trying to solve the same problem. She said categorizing the problem being addressed, looking at the mission and choosing carefully can help determine how best to allocate resources. Another challenge experienced by each panelist was trust. Bretz said it took 14 years for FS-ISAC to build up trust, but he has seen dramatic results

when attacked organizations shared information about an attack and asked for help from colleagues in FS-ISAC or other partner organizations. Kennedy said the industry has a shared customer, but also a shared enemy; so the more trust among its various participants, the better. She added that given what is at stake, the industry prefers to address security issues through collaboration rather than to have legislative interventions.

During the audience discussion, panelists were asked to look ahead, about three years after the implementation of EMV. Questions posed centered on where fraudsters will go after the payments system has been secured and what the focus of private sector collaboration will be. Panelists generally agreed that the industry and technology likely will have changed greatly in three years, perhaps in unimaginable ways. Votaw said she thinks FIDO will still exist in three years, focusing on the same issues. Bretz added that as the industry changes in that time, so will the criminal element, and the payments industry likely will be responding to their innovations. And, if one assumes the payments system has been secured, Votaw said the fraud next would go to where there are weaknesses in the system. O'Malley added the most immediate attack will be on CNP transactions and that current and future targets will be in nontraditional spaces not necessarily thought about from a payments security perspective but that will affect the industry. Kennedy said it is important to be constantly evolving, looking at where fraudsters are going and protecting customers.

## **X. Role of Government in Payments System Security**

In the conference's final session, "Role of Government in Payments System Security," Gordon Werkema of the Federal Reserve Bank of Chicago guided a discussion among U.S. and international public authorities involved in policy initiatives related to deterring payment fraud and/or improving cybersecurity. During the discussion, panelists spoke about the role of government in promoting payments system security and protecting sensitive data and offered insights about the tools that regulatory bodies have at their disposal—moral suasion, regulation, operation and cooperation.

Chrissanthos Tsiliberdis of the European Central Bank (ECB) said the main objective of the ECB is to ensure that the financial market infrastructures (FMIs) are safe and efficient. To accomplish this objective, central banks and other regulators have a threefold task: to keep processes flexible enough to accommodate the pace of innovation, to ensure fair competition

among participants and to require that adequate minimum security requirements are being implemented by service providers. Tsiliberdis shared that the ECB has been actively monitoring the payments market and its initiatives to observe how participants are sustaining the efficiency and safety of the payments systems they provide to the market. He noted that over time, the ECB has observed that monitoring, in some cases, has not been successful. In response, the Eurosystem created SecuRe Pay as a forum to address issues pertaining to the security of online card payments. He mentioned that SecuRe Pay is developing new policies for the cyberresilience of FMIs and retail payments services, cooperating with other banking authorities and will be analyzing and monitoring incidents and fraud reporting. Further, Tsiliberdis shared SecuRe Pay has sanctions authority to deter cyberattacks and formulates/coordinates on legislation on cybersecurity.

Coen Voormeulen of the De Nederlandsche Bank provided insights as chair of the Bank for International Settlements' Working Group on Cyber Resilience, which is comprised of about 20 countries. The working group focuses on systemic risk and cyberresilience of FMIs and publishes guidance for overseers on how to look at FMIs in terms of business continuity, operational risk, legal risk, business risks—risk management in general. Voormeulen noted that while the guidance is for FMIs, it may be applicable in some fashion to systemically important and prominently important payment systems. Voormeulen added that cyber goes much further than information technology. 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. It is important to consider the whole cyberresilience profile of an organization when new services, products or tools are launched. It is important to have a communication plan in place in the event of a crisis. Finally, it is critical to have a business resumption plan for how to resume operations in a safe way, including a recovery time objective. He shared that the work group planned to publish a guidance note in November, to be followed by a two-month public consultation period—for which the world was invited to respond. The Working Group on Cyber Resilience's goal is to publish the guidance note in the spring of 2016.

Anjan Mukherjee of the U.S. Department of the Treasury noted that the payments system as he thinks of it was initially built for connectivity, not for security. Much of the architecture that underlies the payments system is legacy in nature and subject to the rapid technological change. Mukherjee

said Treasury is focused on areas of greatest risk, and given rapid accelerations in Internet use there is a need to be extraordinarily cautious. Toward that end, he said Treasury helped formulate and coordinate the Obama administration's legislative proposals in cybersecurity, which, among other things, looked to facilitate information sharing and data breach notification. He also said Treasury will use its sanctions authority to deter targeted, malicious cyberattacks.

During discussion among the panelists, the point was made that while cyberattacks have no borders, global coordination remains a challenge. Tsiliberdis observed that the optimal way to collaborate varies by country. In some countries, regulators may need to push for collaboration while in others regulatory activity may hinder collaboration. Mukherjee offered that collaboration may be stimulated in many ways, for example FS-ISAC and crisis management exercises. He noted that the biggest struggle is how to implement internationally and suggested that guidance on baseline protections and best practices, information sharing and recovery planning from the National Institute of Standards and Technology may be a useful resource for collaboration. It is a tool that can help bridge differences in cultures—in how issues of payments security are dealt with. Voormeulen added that promotion of cross-border information sharing among FMI's also would be beneficial.

Questions posed by participants to the panel included: What role do you think public authorities play in influencing culture? What is the federal government doing to help encourage various state government entities to follow the federal government's efforts? What role, if any, do public authorities have in supporting or engaging private sector-led initiatives? Voormeulen and Mukherjee agreed it is difficult for public bodies to impose culture, and that at best it is possible to bring parties together and make them aware by sharing information on best practices. Tsiliberdis added that building trust among different participants is a point of emphasis. As for attempts to persuade states to follow the federal government's lead, Mukherjee said that impediments to the federal government's ability to impose standards mean it mostly can help by facilitating discussion and encouraging membership in FS-ISAC. Tsiliberdis added that in supporting private sector efforts, "we always take under consideration what has been developed by the market and will not try to reinvent the wheel."

## **XI. Closing Remarks: Views from the Kansas City Federal Reserve Bank**

Closing remarks were made by Esther L. George, president of the Federal Reserve Bank of Kansas City. George noted that although the Federal Reserve is relatively unique among central banks as an operator of retail payment systems, international public authorities that do not operate retail payment systems have become more active in raising concerns about their security. Some play an explicit role with public mandates while some induce voluntary action. The Federal Reserve has chosen to lead through a collaborative approach, which is not new for the Fed. George reflected that since the founding of the Federal Reserve, observers have looked to it to provide leadership on advancing safety, efficiency and accessibility of the U.S. payments system. Congress initially designed the Fed to serve as a payments system operator through the regional Reserve Banks and as an overseer of the system through its supervision of financial institutions. She said these roles give the Federal Reserve relevant insights as it works with others to address the security challenges of today.

George said that as the Federal Reserve seeks to drive improvement in payments systems through a collaborative approach, two task forces comprised of diverse and committed membership have been convened. One, the Faster Payments Task Force, is focusing on identifying and evaluating approaches for implementing a safe, ubiquitous and faster payments capability in the United States. The other, the Secure Payments Task Force, is providing input on security aspects of a faster payments capability and serves as a forum to advise the Federal Reserve on how to address security matters and to identify and promote actions that can be taken by payment system participants collectively or by the Federal Reserve System.

In concluding, George said she sensed a greater degree of consensus around the security challenges the payments system faces, and noted the challenges are also opportunities to achieve a faster, more secure and widely available payments system in a way that maintains the public's confidence.

## **XII. Conclusion**

Securing the payments system is a matter of utmost importance to payments participants and policymakers. Over the course of this day and half long conference, there was a robust exchange of thoughts and insights about

the need for data collection in standardized forms to better understand rates, prevalence and origination of fraud and security breaches, as well as the costs and benefits of various security strategies. There also was a stated recognition that there is no “one-size-fits-all” solution for securing payments systems; rather a multipronged approach is needed to improve payments security. Technologies such as encryption and tokenization do not compete; they are complementary. Coupled with these technologies that enhance data security or devalue data, stronger payer authentication can be expected to improve payments security. There also was much discussion about collaborative efforts under way in the private and public sectors, both domestic and international, to address payments security. Since payments security is everyone’s concern, deciding between private and public efforts is likely a false dichotomy; instead, the private and public sectors need to work in tandem. These insights will help inform the decision making of central banks, other policymakers, and private sector payment participants as they approach solving the puzzle of payments security.

## Endnotes

<sup>1</sup><http://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>

<sup>2</sup>The Observatory, created in November 2001, is a forum for fostering dialogue and information sharing among all parties in France concerned with the smooth operation and security of card payment schemes. The APCA is a self-regulatory body set up by the payments industry to improve the safety, reliability, equity, convenience and efficiency of the Australian payments system. APCA's 100 members include leading financial institutions, major retailers and other principal payments service providers.

<sup>3</sup>3D Secure is a technology for authenticating the payer of an online purchase, and requires adoption by the online merchant, the acquirer and the card issuer.

<sup>4</sup>The Federal Reserve System's Secure Payments Task Force was convened to engage a diverse array of stakeholders in advancing the work outlined in "Strategies for Improving the U.S. Payment System," published in January 2015. The mission of the Secure Payments Task Force is to provide a forum for stakeholders to advise the Federal Reserve in its leader/catalyst and operator roles on payment security matters, and identify and promote actions that can be taken by payment system participants collectively or by the Federal Reserve System.

<sup>5</sup>The payment account reference facilitates receipt of the PAN for loyalty programs and for fraud and risk. If this information is sent in the clear it defeats the purpose of tokenization.

<sup>6</sup>The American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X9 F6 work group is working on a security tokenization standard that addresses tokens used after initial payment authorization (i.e., post-authorization tokens), such as when an acquirer provides tokenization services to merchants.