Lael Brainard: Building a safer payment system

Speech by Ms Lael Brainard, Member of the Board of Governors of the Federal Reserve System, at the Federal Reserve Bank of Kansas City Conference "The Puzzle of Payments Security: Fitting the Pieces Together to Protect the Retail Payments System", Kansas City, Missouri, 25 June 2015.

* * *

Thank you for the opportunity to speak to you today. I especially want to thank Federal Reserve Bank of Kansas City President Esther George for her leadership in the initiative that has brought us all together here today to discuss improvements to the U.S. payments system. We have a diverse group of professionals participating in this conference, from industry, academia, and government. It takes all of us, working together, to maintain and enhance a safe and secure payment system.

The payment system touches our daily lives, whether it's a consumer paying a bill, a company deciding to upgrade its point-of-sale terminals, a technology startup developing a new peer-to-peer payment app, or the government issuing tax refunds. Americans make more than 120 billion noncash payments each year.[1] But it's only when something goes wrong, like a data breach at a major retailer or bank, that the typical end user takes notice of the payments process.

As the central bank of the United States, the Federal Reserve plays many roles in the payment system, including payment system operator, supervisor of financial institutions and systemically important financial market utilities, regulator, researcher, and catalyst for improvement. Most of you are aware of our current efforts to improve the speed, efficiency, and security of our payment system. I'd like to discuss that project for a few minutes, and then talk about four things that we should all be doing to enhance payment security.

For some years, members of the public have told us with increasing frequency and intensity that they see the United States falling behind other nations in the speed and security of our payment system. We hear all the time that the Federal Reserve should do something about this. But, despite our multiple roles, the Federal Reserve does not have broad authority to simply restructure or redesign the payment system. So, two years ago, the Fed published a consultation paper that sought public input on ways to make the U.S. payment system safer, more accessible, faster, and more efficient from end-to-end.[2] As we evaluated the substantial volume of public comment in response to the paper, the Fed also conducted research; met with a wide set of stakeholders, including banks, merchants, technology companies, consumer organizations, and others; and worked to enhance our own payment services.

Building on this work, we released a second paper earlier this year, entitled "Strategies for Improving the U.S. Payment System."[3] This paper synthesizes a range of views and presents a multifaceted plan for collaborating with payment system stakeholders to enhance the speed, safety, and efficiency of the U.S. payment system. The paper emphasizes the need for a secure payment system that has the public's confidence and that keeps pace with the rapidly evolving and expanding threat environment.

To facilitate cooperation among the many stakeholders, under the leadership of Esther George, we have established two task forces: one for faster payments and one for payment

---

1 Federal Reserve System (2014), "The 2013 Federal Reserve Payments Study: Summary Report and Initial Data Release (PDF)

2 See Federal Reserve Banks (2013), "Payment System Improvement – Public Consultation Paper (PDF).

3 See Federal Reserve System (2015), "Strategies for Improving the U.S. Payment System (PDF)."

security. These task forces will work both independently and in concert. The security experts on the secure payments task force will advise members of the faster payments task force as they identify effective approaches for implementing faster payment capabilities. The secure payments task force also will advise the Fed on payment security matters, and determine areas of focus and priorities for future action to advance payment system safety, security, and resiliency.

I am pleased to report that we are off to a great start in the months since the "Strategies for Improving the U.S. Payment System" paper was released. More than 300 participants from a range of stakeholders signed up to be part of the faster payments task force, and more than 200 joined the secure payments task force. These task forces have chosen, or are in the process of choosing, members to serve on their respective steering committees, which will help guide the task forces' efforts.

Earlier this month, the faster payments steering committee met to begin developing timelines, processes, and criteria – including criteria related to security – that will be used to evaluate potential approaches to improving the speed of the payment system. Last week, the full task force met to continue the work. I am told that they had a great meeting – everyone was interested, engaged, and eager to get to work. The secure payments task force conducted its first organizing call earlier this month and, in mid-July, its steering committee will meet for the first time. Momentum is growing. By the end of next year, the plan is for the faster payments task force, with input from the secure payments task force, to have laid out its detailed thinking on the most effective approaches for implementing faster payments in the United States. Then, it will be up to the industry to implement these approaches.

But, before we reach the finish line, the task forces will have to wrestle with some tough issues related to payment security. I would now like to talk about building a safer payment system. I'll start with two brief stories.

First, let me take you back to the 1960s, when paper checks were the dominant noncash payment method and were sent by plane or truck to be cleared. A man walks into a bank with a payroll check. A teller cashes the check. A few days later, the man returns. The teller recognizes him, and is happy to cash more checks. The checks are fraudulent, but the teller doesn't know that. The man knows that the string of numbers encoded on the bottom of the check determine the geographic area where the check will be drawn. So he creates a fake check with a routing number that will send that paper check across the country. Because the teller recognizes the man when he comes back, the teller feels comfortable cashing the second round of checks because the first check has not yet been returned. By the time the bank realizes the checks are fraudulent, the man is gone. Some of you will recognize that man as Frank Abagnale, former con artist and now a security consultant.

Now, fast-forward 50 years to 2013. A man walks up to an ATM with a prepaid debit card. He types in a PIN and withdraws a large amount of cash. But it's not just one man: there are many individuals doing the same thing at thousands of ATMs in dozens of countries. The cards are counterfeit, but no one has detected that yet. Over the course of ten hours, the individuals withdraw $40 million in cash. How does this happen? Before the thieves walk up to the ATMs, hackers break into a payment processor's database, steal a small number of prepaid card account numbers, and raise the cards' withdrawal limits. They then distribute counterfeit cards to "cashing crews" around the world who make the withdrawals.

These well-known payment fraud schemes were perpetrated in different eras, and juxtaposing them highlights how the payment security landscape has changed. Frank Abagnale relied on the slow speed of the paper check-clearing system and in-person social engineering. In contrast, the ATM thieves relied on rapid transmission of data to remotely steal account information and alter withdrawal limits, all without interacting with bank employees. Today, fraud can be executed quickly, perpetrated on a massive scale, and carried out remotely.

In light of this new environment, I will suggest four things that all of us ought to be doing with respect to payment security. Some are already being done. Too often, though, such efforts are overlooked or inconsistently applied.

1. Safe innovation

This is an exciting time for the payment system. Technology companies are creating new methods to pay with mobile phones and even wearable devices. Banks are building faster payment capabilities into their deposit account systems. Banks, payment card networks, and merchants are rolling out Europay, MasterCard, and Visa (EMV) chip cards and using compatible point-of-sale terminals. Many of the newest products in the market are impressive, incorporating new technologies like biometrics and tokenization. End users and the media have taken notice.

History shows that we should embrace innovation. Technological innovation has continually pushed the payment system forward. Payment cards, both credit and debit, are an example. Thirty years ago, everyone carried cash. Today, young adults increasingly prefer to rely on cards and mobile phones. Payment cards have improved convenience and security in certain ways, like reducing the impact of a stolen wallet.

But history has also shown that new technologies must be adopted in a prudent fashion. Technological innovations can provide substantial benefits to payment system efficiency and security in the long run, but they often introduce new, unanticipated risks. For example, although payments cards reduced the impact of a stolen wallet, they've also introduced new risks, like counterfeit card fraud. It is important that we identify and address the unanticipated risks that inevitably result when we try new things. These risks may be tolerable in the short run, so long as we work to identify, prevent, and mitigate them early on in the design and implementation process. In the case of payment cards, over time, technologies have been broadly implemented to mitigate many of the risks. For instance, computer algorithms now analyze transactions in real time and can prevent the same card number from being used to make purchases in Washington, D.C. and in Kansas City five minutes apart.

We also need to consider the complexity of the payment system. It is a vast network with millions of endpoints and a wide variety of participants. Many innovators do a good job of incorporating advanced security features into their individual products. But new products also need to be securely integrated into the payment system as a whole.

To innovate safely, payment system participants must work together by participating in coordinated efforts to improve the payment system. At a minimum, banks, merchants, and other institutions that process or store sensitive financial information need to keep their hardware and software current to the latest industry standards. Network operators and standards-setting bodies play an important role by identifying these standards and coordinating their adoption among network participants. The EMV rollout that is taking place right now is a good example.

The market should be the primary driver of change, and government should avoid stifling healthy innovation. But policymakers can play a role by actively listening to concerns from the public regarding barriers or gaps in regulatory regimes that may create disincentives for developing new, safe products. Policymakers can also bring industry participants together. The task forces that were created as part of the Fed's payment system improvement effort bring together a wide range of payment system participants to sit at the drafting table to create a blueprint for a safer and more efficient payment system.

Complacency is everyone's enemy. Unfortunately, the firms involved in the payment system are not the only ones innovating: criminals have an ever-increasing arsenal of cyberweapons at their disposal. That brings me to my second point.

2. Prevention

You will be attacked. Criminals today are often motivated, intelligent, well-organized and well-funded. They also have varied interests: some seek financial gain, while others hope to disrupt our nation's financial institutions and payment system. What should we be doing to prepare? One clear area of focus needs to be on implementing preventive tools, or simply put, defensive tactics. You won't survive the game if you don't play good defense**.**

The deployment of EMV chip cards in the United States represents an important step forward. But we should not stop there. For many years, traditional authentication methods like signatures and static passwords have been used to verify that an individual is authorized to initiate a payment. New approaches to authentication increasingly offer greater assurance and protection. Given the current technologies that we have at our disposal, we should assess the continued use of signatures as a means of authenticating card transactions.

It is important to layer security tools and procedures. Methods to devalue payment data, like tokenization and encryption for data at rest, in use, and in transit, mitigate the effect of a data breach. Analytics can identify and prevent fraudulent transactions. Firewalls and segmentation of technology supporting critical functions can protect networks from outside attacks.

Also, remember that people inside your organization and organizations that you work with can pose a significant risk. One study found that more than 20 percent of security incidents could be attributed to insiders.[4] Segregation of duties, background checks, and monitoring for anomalies help reduce the risk of insider threats. Strong vendor-management programs can reduce risks from an institution's partners and service providers.

3. Planning

As crucial as they are, we should keep in mind that these prevention tools cannot stand alone. Even with stronger authentication methods, robust network security, and other approaches in place, preventive measures aren't sufficient to manage security risks. Such measures are designed to protect against known risks. But those looking to exploit the system will continue to devise new methods of attack. In some of the recent high-profile data breaches, companies have scrambled to deal with the aftermath. This brings me to my third point. We need a comprehensive way to think about planning. The National Institute of Standards and Technology's cybersecurity framework is one of many voluntary cybersecurity frameworks that provide a holistic, risk-based approach to planning.[5] In addition to preventive measures, the framework identifies four additional core functions: identify, detect, respond, and recover. We can apply these four functions to securing the payment system.

An important first step is to identify internal business processes and assets, as well as external threats. You can't protect yourself unless you understand how your business is structured. This sounds simple enough, but an organization's computer systems are often unexpectedly interconnected. Some of the largest point-of-sale data breaches, for example, originate outside payment card systems.[6] You should also keep up to date on cyber developments and gather information about threats from information sharing forums, including FS-ISAC, US-CERT, and the FBI's InfraGard.

Regardless of how well we identify and protect, we also need to plan for a potential attack. To address this, the NIST framework calls for plans to detect, respond, and recover. Victims

---

4 Verizon (2015), "2015 Data Breach Investigations Report," www.verizonenterprise.com/DBIR/2015

5 See National Institute of Standards and Technology (2014), "Framework for Improving Critical Infrastructure Cybersecurity (PDF)."

6 Verizon (2015), "2015 Data Breach Investigations Report," www.verizonenterprise.com/DBIR/2015.

are often not aware that they've been breached. Did you know that last year the median amount of time it took to discover a breach was about 200 days?[7] Plans need to include methods to detect attacks. You also need to have a response plan. If your point-of-sale system is compromised or your account records are stolen, do you know which law enforcement agencies you should work with? You will be more effective containing the impact if you have thought through the necessary responses beforehand. Finally, you need to have plans in place to recover business functions. This may include investments in new tools and approaches to aid in rapid recovery. I would also advise that you participate in industry-led tabletop exercises to help you think through how to respond and recover from cybersecurity events.

4. Education

We've talked a lot about fostering the security of the payment system, but we should also talk about the public's perceptions. Even if we have a comprehensive, well-implemented security plan, one high-profile breach can shake public confidence. Research suggests that the way consumers feel about a particular payment mechanism affects the way they choose to pay. For example, the Federal Reserve's most recent report on consumers' use of mobile financial services notes that security concerns are a main impediment to the adoption of mobile financial services.[8] Education is a way to enhance both payment system security and public confidence.

My fourth point is that, collectively, we could do more to empower consumers to use financial products safely by educating them on the risks they face and the steps they can take to protect themselves. For example, financial institutions can provide and help customers understand online banking tools like credit card transaction alerts that can help consumers spot or stop fraud. We also need to be prepared, to the extent possible, to respond to a security incident in a transparent and timely manner so that consumers understand the implications of the event. Policymakers can also provide facts and data to paint a realistic picture of the threats that exist in the payment system. One example is the Federal Reserve's triennial payments study, which presents statistics on fraud for the largest retail payment systems that could be used by companies and the media when explaining risks to consumers.[9]

Knowledge is power. Education is critical to fostering the security of the payment system and, ultimately, to maintaining public confidence.

Conclusion

The things I've discussed today apply to all payment system participants. Each of us has an important role to play in building a safer payment system. Given the payment system's complexity, it's important to keep in mind that we all need to work together when we innovate, prevent, plan, and educate.

I want to close by asking for your support. With our payment system improvement effort in full swing, now is the perfect time for payment system participants to come together to build a safer and more efficient payment system. If you've joined one of our task forces, I hope that you will maintain a high level of engagement. If you haven't, I encourage you to do so, or at

---

[7] Mandiant (2014), "M-Trends 2015: A View from the Front Lines," www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf.

[8] Board of Governors of the Federal Reserve System (2015), "Consumers and Mobile Financial Services 2015 (PDF)."

[9] See Federal Reserve System (2014), "The 2013 Federal Reserve Payments Study: Detailed Report and Updated Data Release (PDF).

least to follow their progress. We will continue to seek input and provide updates through live and virtual forums, surveys, industry- and Federal Reserve-sponsored groups and events, and online feedback mechanisms. Thank you to the Federal Reserve Bank of Kansas City for organizing this conference and to all of you for participating.