EMBARGOED UNTIL Friday, January 30, 2015
at 2:45 A.M. U.S. Eastern Time and 9:45 A.M. in Cape Town, South Africa
OR UPON DELIVERY

"Cyber Security and Financial Stability"

Eric S. Rosengren
President & Chief Executive Officer
Federal Reserve Bank of Boston

Remarks at forum on
"Strengthening Financial Sector Supervision and Current Regulatory Priorities"
organized by
the Basel Committee on Banking Supervision
and the Financial Stability Institute

Cape Town, South Africa
January 30, 2015

"Cyber Security and Financial Stability"

Eric S. Rosengren
President & Chief Executive Officer
Federal Reserve Bank of Boston

Remarks at forum on
"Strengthening Financial Sector Supervision and Current Regulatory Priorities"
organized by
the Basel Committee on Banking Supervision and the Financial Stability Institute

Cape Town, South Africa
January 30, 2015

Good morning. I would like to thank Josef Tosovsky, chairman of the Financial Stability Institute of the Bank for International Settlements, for inviting me to speak at this forum. The Institute serves an important role by increasing awareness of financial stability issues and highlighting actions that can be taken to address vulnerabilities.

Today I am pleased to speak with you about a very important topic – cyber security for banks, payments systems, and central banks – and its implications for financial stability. As I begin, I would note as I always do that the views I will express today are my own, not necessarily those of my colleagues on the Federal Reserve's Board of Governors or the Federal Open Market Committee (the FOMC).

As we all know, innovations in computing and communications technologies are rapidly altering the landscape of payments. And overseeing the safety, security, and efficiency of payment systems is a major responsibility of many central banks. Indeed, I would argue that for central banks, the transmission of monetary policy, the provision of services to financial intermediaries, and the supervision of the banking system are integrally linked.

However, payment systems are becoming less bank-centric and are changing much more quickly than their regulatory framework. As payment systems quickly evolve with new technologies, a potentially serious financial stability concern is inherent in cyber security. So, today I am going to describe why I view cyber security as one of the most serious financial stability concerns facing central banks, and why we need to become more directly involved.[1]

By way of example, consider the many payment choices available to a consumer when simply purchasing a shirt. The consumer can go to the store and use cash, a debit card, a credit card, a prepaid card, or even a mobile phone. Alternatively, the shirt can be purchased on the Internet, the consumer paying with a credit card or signature debit card, PayPal, direct debit from a bank account, or alternatively using a mobile app such as Apple Pay or Google Wallet.

Each of these transaction options would involve combinations of different payment systems, intermediaries, and technologies. Because these options ultimately ride on traditional banking and payment "rails," consumers see little need to consider whether the behind-the-scenes technology, accounting, and bookkeeping functions are truly available, safe, and secure.

Despite the advantages to consumers and businesses from rapid innovation in payments systems, cyber-security issues are beginning to intrude. Cyber crime has directly affected millions of consumers.[2] The value of stolen data has grown exponentially with the evolution of a very sophisticated black market for personal information.[3] All this highlights one of the economic risks of moving to electronic payments – a wide (and growing) variety of entry points for those looking to steal, divert, or disrupt payments.

When financial gain is the primary motivation behind the fraud, there are three options for containment. First, prevent the intruder from entering the system. Second, and often more importantly, prevent the intruder's ability to *leave* the system with confidential data. Or third, devalue the data so it is meaningless to an intruder who gains access to it.

News media have reported thefts involving consumers' credit card information. To date, these incidents have not resulted in systemic shocks to the economy or to payments networks. Still, should breaches continue, a lack of confidence in traditional payments may lead people to less efficient options. Likewise, while these events do not really introduce systemic risk from a total-dollar-value perspective, they nonetheless

contribute to the erosion of confidence in payment mechanisms and ultimately increase overall transaction costs.

A more serious case would be an attack on payment systems aimed at disrupting transactions, for example by a rogue state or entity. Prevention is difficult because the attacker does not need to "enter" the system to be disruptive, and there is no need to exit with confidential data – all the attacker needs to do is flood the public-facing "front door" of a payments processor with enough traffic to make the system unavailable.[4] However, the bad actors are moving on to much more nefarious ways of penetrating processing assets.

Preventing disruption puts an emphasis on ensuring that resiliency, monitoring, detection, and recovery capabilities are designed into, and operational in, any payment system. An attack on payment systems that renders consumers and businesses unable to transact business could be extremely disruptive and could possibly cripple an economy. To that end, the adoption of a national defense grade security level, rather than a commercial grade security level, would mean a much more resilient – albeit expensive – payment system.

Today I will briefly discuss how complex our payment system has become, and consider susceptibility to cyber-related interruptions. I will then discuss the financial stability concerns inherent in current arrangements. As an example, I will discuss the payment disruptions that occurred after the terrorist attacks of September 11, 2001. I will mention some steps that need to be taken, some specific actions being taken by the Federal Reserve Bank of Boston, and a recent report issued by the Federal Reserve.

I. Payments Systems

There are a variety of payment systems in the U.S., and the volume and dollar-value of the transactions that flow through them is striking. The 12 regional Federal Reserve Banks collectively process over $4 trillion in payments *every day*.[5] However, the U.S. payments landscape encompasses much more than those processed by the central bank. In the realm of so-called "retail" payments, there are a variety of payment systems or networks that directly support credit and debit card payments as well as Automated Clearinghouse (ACH) payments, and that indirectly support intermediaries such as PayPal, Google Wallet, or Apple Pay. There are also payment systems devoted to "wholesale" funds transfers, including Fedwire Funds transfers, Fedwire Securities transactions, and the Clearing House Interbank Payments System or CHIPS.[6,7] Other systems focus on securities transfers and payments related to stocks, bonds, options, and derivatives.

It is perhaps easiest to consider cyber crime in the context of a generic retail payment, as shown in **Figure 1.** The consumer can choose from a variety of payment methods and platforms[8] to initiate a transaction. The transaction information and payment method then enter the merchant's computer system. For a credit or debit account payment, the merchant (or third-party processor or "acquirer") transmits the account information to the issuing entity for authorization. The issuing entity approves (or rejects) the authorization back through the processor to the merchant. The payment involves the issuing entity or its bank sending funds to the merchant's bank, with settlement on the books of the Fed.

At each stage of the transaction, a different party may have customer information – which, if stolen or destroyed, could impact other parties to the transaction. At the point of initiation, the consumer could be tricked into providing account information, or during processing any of the institutions could expose the customer's information to a third party.[9]

Fraudsters have typically targeted consumer payments, making them a critical area for focus – and one where large-scale hacking incidents have been well-publicized. Should fraud become so widespread that customers lose confidence in the safety of payment transactions, the entire payment landscape (both retail point-of-sale and e-commerce) could be severely impacted and entire transaction models could be imperiled.

Unfortunately, the retail space is only one area where cyber-security breaches could impinge on payment systems. **Figure 2** shows the U.S. regulatory arrangements covering payment, clearing and settlement systems. As the figure illustrates, payment systems extend well beyond retail payments to other areas also susceptible to cyber-security problems.

Arguably, the complicated payment structure[10] is actually something of an advantage in that the payment system is decentralized. Without a single point of failure, problems in one area may not directly impinge on other areas – at least not immediately.[11] But, with diffuse roles and responsibilities in the payments landscape, involving both the private and public sectors – and with attackers looking for the weakest link – a unified cyber-prevention approach is difficult to implement. The complex landscape means a significant investment is required to protect the many potential points of failure. Also, complexity makes it difficult to react in a more coordinated fashion to

concerns. A particular worry relates to attacks where the purpose is not financial gain, but rather disruption of payment systems and economic activity.

II. Disruptions of Payment Systems

The attacks on September 11, 2001 had impacts beyond the tragic loss of life and massive destruction of property – including impacts on payment systems. Because the World Trade Center was located near Wall Street, numerous payment systems were affected. Insufficient resiliency became clear – for example, the New York Stock Exchange halted trading for four days. The flow of funds through the banking system was also impacted.[12] Some banks did not have sufficient back-up systems and could not receive incoming funds. This resulted in some banks having a surplus, while others found themselves short of funds or reserves.

Figure 3 shows the dramatic increase in the volume of federal funds (Fed Funds) and Discount Window loans that occurred as banks tried to reallocate funds or reserves around the payment system during that period. Work by McAndrews and Potter[13] on the liquidity effects of the events of September 11 documents that both the value and volume of Fedwire activity declined by well over 20 percent, as some banks had difficulty communicating with customers and counterparties, and some institutions lost the ability to track the flow of funds.

Within a week, most payment flows had been restored. Banks were able to re-create files and restore lost infrastructure. In addition, actions taken by the Federal Reserve facilitated recovery – the Federal Reserve not only helped restore financial communications, but also waived overdraft fees, actively encouraged borrowing from the

Discount Window, and conducted open market operations to increase reserves in the banking system.

In reaction to the disruption, significant longer-run actions were taken. The *Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System*[14] required fundamental changes to prevent a similar shock from having a large impact in the future. Payment systems and financial institutions made costly improvements that dramatically improved the speed at which payments activities could be restored.

With September 11, the implications of physical damage became fully evident. The corrective activities focused on geographic dispersion, and resiliency for a physical event. In contrast, a cyber-attack could have greater scale and take an extended period of time to play out prior to the full impact being known. And adversaries are well funded, and have time to evaluate and plan. We need to consider and protect against many and all types of attacks, while adversaries need just *one* vulnerability – and we must assume they are always trying.

While the payment disruptions that followed the September 11 attacks were not related to cyber security, there are analogies and lessons that can be applied to a more proactive and coordinated approach.[15] Underlying infrastructures need to better ensure that payment providers take sufficient precautions to minimize the likelihood and impact of cyber attacks – whether commercially motivated or focused on disruption. This will require a level of information-sharing and expectation-setting by national defense agencies, regulators, supervisors, and operators exceeding that of today's very fragmented but dynamic payment systems.

In the U.S., legislation aimed at improving the way information is shared among the public and private sector has stalled due to privacy and other liability concerns. However, the Obama administration has noted that cyber threats are "one of the most serious economic and national security challenges we face as a nation"[16] and is promoting legislation to require enhanced threat information sharing among the two sectors.

III. Addressing Cyber Security

In addition to addressing cyber security with a more integrated and holistic approach among the large payment systems operators, there is work that central banks should be considering on the local and smaller-scale levels. **Figure 4** highlights some of the significant cyber-security problems that have been experienced by major business entities as a result of their suppliers or sub-contractors being compromised. Often, it seems, the initially-compromised organizations tend to be smaller and less sophisticated, and may not have sufficient resources to protect against a hacker intent on using the weakest link to penetrate a computer system that reaches, and could impact, other entities and systems.

In the United States we have over 6,000 banks, and many are small institutions with modest information technology teams who often have job responsibilities beyond cyber-security. These smaller financial institutions do not have regular access to national security briefings and often rely on outside vendors or third-party processors, many of whom may also be relatively small organizations with limited cyber-security capabilities. Despite their best efforts, such institutions may provide determined intruders the least

technically advanced defenses and easiest entry points into payment systems. So bolstering the awareness and defenses of these sorts of smaller organizations should be a priority.

Sharing actionable information about cyber attacks has the potential to significantly improve a firm's preparedness. Some larger institutions have committed to share cyber-threat information in a more real-time manner, or through industry collaboration forums such as the Financial Services-Information Sharing Analysis Center[17]. Still, many government agencies and cyber-security firms are reticent to share information and discuss problems because of potential legal liabilities, or reputational risk concerns.

In 2014, the Federal Reserve Bank of Boston began a pilot program focused on the sharing of cyber-threat information by, and among, small- to medium-sized banks. This pilot, for a specific segment of a single industry, was very successful. We intend to expand the program in 2015. Importantly, the program is not part of our supervisory oversight of banks, but instead is conducted by Boston Fed cyber-security experts, who can share information about emerging threats and mitigants. All participants sign a non-disclosure legal agreement that stipulates that the information provided is shared for the sole purpose of allowing members to improve their own cyber defenses, and cannot be used for any other purpose.[18] While still in the early stages of implementation, the initial results are encouraging. The experience to date highlights that more peer sharing for groups of smaller institutions has the potential to help thwart cyber criminals' potential entry to the payment systems.

Similarly, the Boston Fed is a founding member of the Advanced Cyber Security Center (ACSC), a nonprofit organization that brings together industry, university, and government organizations to address the most advanced cyber threats. A key focus is sharing cyber threat information. The Boston Fed facilitates monthly "Cyber Tuesdays" to enable discussion among security practitioners on emerging issues and the state of the cyber threat environment.

And earlier this week, the Federal Reserve System issued a paper on *Strategies for Improving the U.S. Payment System*.[19] A key strategy highlighted in the paper involves working "to reduce fraud risk and advance the safety, security and resiliency of the payment system." The paper notes the Federal Reserve belief that security is the foundation of any payment system, and our intent to work with a wide range of stakeholders to promote an environment where end-to-end payments security preserves privacy and integrity, commands high public confidence, and improves continuously in response to evolving threats. The paper has a somewhat different focus, but complements, what I've talked about today.[20]

Concluding Observations

Cyber security is a serious financial stability concern. The potential for loss of trust in payment systems due to incursions or disruption is a key consideration. Beyond intrusions with financial motivation, the increased activity of rogue states or entities in what is essentially cyber warfare or cyber terrorism changes and elevates the nature of the protections necessary.[21]

In general, central banks need to focus on how best to address this emerging concern and play a proactive role in assuring the cyber resiliency of payment systems. Given privacy and secrecy concerns, open communication of threats and mitigants is often problematic. And as I discussed today, the rapid technological evolution of payment systems has resulted in a highly fragmented and diffuse regulatory framework. There are serious challenges and obstacles to comprehensive solutions. Central banks are essential to this discussion and to the progress that needs to be made. And given the importance of a safe and available payment system to the functioning of a nation's economy, investment in core aspects of systems to ensure they are as secure and cyber resilient as possible must be a national priority.

Our efforts cannot focus solely on preventing incursions, because almost certainly someone will ultimately breach many cyber defenses. The focus should also be on rapid detection, limiting damage, and rapid remediation of damaged resources.

Because the weakest link provides the greatest opportunity for intruders, focusing solely on the largest players is unwise. Whether a financial institution is located in Northern Maine or near the tip of South Africa, cyber threats know no borders – and neither geography nor small size insulate institutions, and the payment systems that they are part of, from risk. There are opportunities for central banks to play a more active leadership role in this area.

Thank you.

NOTES:

[1] Cyber security risk is well understood. For example, The Bank for International Settlements' Committee on Payments and Market Infrastructure has highlighted the need for more cyber readiness for financial market infrastructures, and the Federal Financial Institutions Examination Council (FFIEC) has a working group focused on raising regulator awareness and improving bank supervision of cyber risk – but actionable items are lacking and the Federal Reserve's Financial Advisory Council has highlighted the need for more sharing of information.

[2] Many consumers with credit or debit cards have experienced the downstream effects of cyber crime. These include the irritation and hassle of a card transaction being denied, or having cards frequently replaced, or having one's personal information or payment identity stolen, or seeing fraudulent transactions that cause financial or reputational harm.

[3] The hackers are no longer just using the information themselves, but selling it to criminal computer scientists and "quants" that correlate it with other stolen data to make it even more valuable.

[4] Many low cost or free automated tools for doing so are, unfortunately, available – even to unsophisticated attackers.

[5] A number equivalent to almost 25 percent of *annual* U.S. GDP

[6] See http://www.newyorkfed.org/aboutthefed/fedpoint/fed36.html

[7] An example of a wholesale payments problem was the system disruption of the Bank of England's Clearing House Automated Payments System (CHAPS) which went down for technical issues and resulted in the disruption of 2,450 home sales.

[8] Such as a credit card, debit card, mobile phone, or computer.

[9] Javelin Strategy and Research estimates fraud losses from bank and credit card accounts was $16 billion last year, up 45 percent from the previous year. However, this probably underestimates the costs of forensic work, law enforcement activities, fraud monitoring, and additional system changes taken to avoid repetition of the problem.

[10] E.g., the complex operating structure, the multi-faceted regulatory environment, and diffuse governance.

[11] Although, as we witnessed in the financial crisis with subprime mortgages and products like collateralized debt obligations, systemic issues can develop across intermediaries based on indirect factors, such as a loss of confidence – as happened to Lehman Brothers and AIG.

[12] While wholesale funding was most impacted, the influence on consumer confidence was important. In some areas, runs on ATMs occurred.

[13] See http://www.ny.frb.org/research/epr/02v08n2/0211mcan/0211mcan.html

[14] See http://www.federalreserve.gov/boarddocs/press/bcreg/2003/20030408/default.htm

[15] i.e., not waiting until a significant intrusion has wreaked havoc for one or more payment systems.

[16] See http://www.whitehouse.gov/the-press-office/2015/01/13/remarks-president-national-cybersecurity-communications-integration-cent

[17] FS-ISAC

[18] This allows for the open sharing of certain limited confidential information that can be used by fellow members to improve their cyber security. By the way, we have found that in-person meetings are most productive in this regard, rather than audio or video calls. In-person meetings allow a trusted network to develop over time. We have found that audio calls do not work as well, because some participants are not entirely comfortable with who else might be listening in.

[19] https://fedpaymentsimprovement.org/wp-content/uploads/strategies-improving-us-payment-system.pdf

[20] The paper notes that "protection against, prevention of, or elimination of cyber attacks, *in general*, is an important topic, but one that is beyond the scope of this desired outcome" [emphasis added]. The paper does however address cyber security as it relates to payment transactions and payment systems.

[21] Indeed, some data indicate a shift of cyber-related events away from financially motivated activity to activity by rogue states, entities, or individuals looking to cause disruption of critical infrastructure, in order to advance a specific agenda.