Michelle W Bowman: Welcoming remarks - Midwest Cyber Workshop

Welcoming remarks (virtually) by Ms Michelle W Bowman, Member of the Board of Governors of the Federal Reserve System, at the Midwest Cyber Workshop, organised by the Federal Reserve Banks of Chicago, Kansas City and St. Louis, 15 February 2023.

* * *

Good morning. It is a pleasure to join you, and I appreciate the invitation to speak to you virtually for this inaugural Midwest Cyber Workshop hosted by the Federal Reserve Banks of Chicago, Kansas City, and St. Louis.[1]

Cyberattacks threaten businesses and consumers everywhere-none of us is beyond the reach of those that initiate these attacks. Community banks have been the target of cyber and ransomware attacks, and they frequently name cybersecurity as one of the top risks facing the banking industry. In my conversations with bankers, some note the difficulty in attracting and retaining the staff needed to mitigate cyber risks. While there are no easy solutions in the defense against cyberattacks, close coordination among all of the groups represented at this conference is a good first step.

As I consider the Federal Reserve's role in supervising cybersecurity, it is important to identify where our engagement can be most effective to enhance the security of our regulated entities. Our efforts must be focused on both banks and their third-party service providers.

In my remarks today, I will briefly discuss four topics. First are the implications of evolving technologies and their impacts on the cyber risk landscape. Second, I will discuss how customer demand for innovation and personalized products has increased reliance on third parties. Third, I will cover the recently effective computer security notification rule, and how that rule can benefit regulators through notification of cyber incidents and banks in monitoring their third-party service providers. And finally, I will briefly address some of the Federal Reserve's recent actions related to cyber risk.

Evolving Technologies and Their Associated Risks

I'll begin with technology and the risks presented by the implementation and integration of new technologies. As the pace of technology innovations continue to accelerate, companies are engaging in business in new ways. New products and services present new risks.

Since the COVID-19 pandemic, we have seen greater interest in customer adoption of digital banking products and utilization of remote work tools by bank employees, both of which have created new opportunities for cyberattacks. Some of these risks are best addressed directly by the bank with assistance from law enforcement, if necessary. Other risks may best be addressed by service providers.

Ransomware
One of these risks is from ransomware, which continues to be an prevalent threat to

financial institutions. Reports of these kinds of attacks have increased significantly over the past five years, with the Financial Crimes Enforcement Network (FinCEN) reporting more than 1,400 ransomware-related Bank Secrecy Act filings in 2021, worth nearly $1.2 billion. This represents a nearly 200 percent increase over 2020 and coincides with elevated geopolitical risk. Moreover, the frequency of ransomware attacks has escalated due to the emergence of ransomware-as-a-service, enabling easier deployment of these types of attacks. Although ransomware impacts financial institutions of all sizes, it disproportionately impacts smaller banks that may not have sufficient resources to protect against these attacks.[2]

Ransomware is often delivered through phishing emails or through the unauthorized installation of malicious programs onto an organization's systems, known as "drive-by-downloads." These tactics take advantage of those with access to a bank's internal systems, whose actions, while perhaps well-intentioned, enable the ransomware cyberattack to occur. According to the Cybersecurity and Infrastructure Security Agency, eight out of 10 organizations had at least one user fall for a phishing attempt, and one out of 10 phishing emails resulted in a user opening a malicious attachment or accessing a malicious internet link.[3] Banks regularly perform exercises testing employee vulnerability to these kinds of targeted attacks. Banks should continue efforts to educate those with systems access about these risks.

Ransomware attacks can be mitigated by bank management. By using a robust, formal risk assessment process, bank management can develop a comprehensive action plan to prevent a ransomware attack from occurring, or to reduce the impact on the bank should such an attack occur. Banks that have planned ahead for a ransomware attack will be better positioned to respond when an attack occurs.

Use of Internal and External Applications

Software and public-facing applications are also potential targets for exploitation, requiring effective planning and implementation of patch management to address emerging and existing vulnerabilities. Hackers constantly seek opportunities to exploit software holes and risks exist even with a bank's best efforts to install the most up-to-date security patches. For example, often when vulnerabilities are identified, providers have not yet provided patches to address these issues, leaving the bank vulnerable to what is referred to as zero-day exploits. Supply chain attacks, like the SolarWinds incident, occur when a bad actor compromises software, or software updates, before the vendor can provide it to customers for installation. While there are some mechanisms to mitigate the risk of these attacks, defenses are limited because organizations rarely control their entire software supply chain.[4]

This is an example of a threat that a bank on its own may not be best equipped to address. Therefore, regulators should carefully consider the appropriate entity for the focus of regulatory attention.

Third-Party Risk Management

Customer demand for innovative and personalized products and services has increased community banks' reliance on third-party relationships to enable them to provide new

technologies. These relationships position small banks to remain competitive and demonstrate their commitment to serving the needs of their customers and communities. At the same time, greater reliance on third parties could create additional opportunity for cyber criminals. The federal banking agencies recognize the increasing role third parties play in providing banks with a multitude of services including access to new technologies, human capital, delivery channels, products, services, and markets. In July 2021, in recognition of this trend, together the Federal Reserve Board, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency jointly released proposed interagency guidance for the risk management of third-party relationships. Although each of these federal banking agencies had already published separate third-party risk management guidance, the intent of the additional proposed guidance is to create consistency across the regulatory agencies and to consider whether further risks should be considered, given the evolving nature of the industry.[5] The banking agencies are currently in the process of considering the comments received on that proposal.

A bank's use of third parties does not diminish its responsibility to oversee those activities in a safe and sound manner and in compliance with applicable laws and regulations, including consumer laws. To assist banks in their oversight of third parties in implementing risk management programs, in 2021 the Federal Reserve began providing state member banks with reports relevant to their third-party partners. These reports contain information that may provide helpful insight in assessing the performance of bank service providers, depending on the services used and the risk the services pose. As a former banker, I see this as a valuable resource; having access to these supervisory reports helps to ensure that banks are receiving the information necessary to most effectively manage exposure to the risks posed by their service providers.

In August 2021, the agencies also released a guide for community banks titled "Conducting Due Diligence on Financial Technology Firms." This guide was drawn from existing guidance, and, while voluntary, it is intended to be a helpful resource for community banks when performing due diligence on prospective relationships with fintech companies.[6]

The third-party service provider landscape has continued to evolve and expand. As a result, we should consider the appropriateness of shifting the regulatory burden from community banks to more efficiently focus directly on service providers. The Bank Service Company Act gives the federal banking agencies significant regulatory authority over outsourced banking services. In a world where third parties are providing far more of these services, it seems to me that these providers should bear more responsibility to ensure the outsourced activities are performed in a safe and sound manner. The computer security notification rule is one example that makes appropriate use of this authority.

Computer Security Notification Rule

Given the escalating frequency and severity of cyberattacks, the agencies published a final rule in late 2021 establishing computer-security incident notification requirements for banks and, importantly, also for their service providers. The rule requires a bank to notify its primary federal regulator as soon as possible but no later than 36 hours after

the bank determines that an incident requiring notification has occurred. An incident requiring notification is defined as a computer-security incident that disrupts or degrades, or is reasonably likely to disrupt or degrade, the viability of the banking organization's operations, resulting in customers being unable to access their deposits and other accounts, or impacting the stability of the financial sector.

In addition, this rule requires a bank service provider to notify a bank-designated point of contact at each affected customer bank. The notification must occur as soon as possible after the service provider determines that a computer-security incident has occurred that materially disrupted or degraded, or is reasonably likely to disrupt or degrade, covered services provided to the bank for four or more hours. Since community banks are largely reliant on bank service providers, the notification requirement is meant to assist in the process of a bank's assessment of the severity of the incident, including the breadth and depth of impact and the necessity to implement internal response protocols. This rule is also a good example of efficient regulation, since bank service providers are often best positioned to identify computer-security incidents.

Since May 2022, banks and bank service providers have been required to comply with the computer-security incident notification rule. The Federal Reserve continues to expect banks to report breaches of sensitive customer information consistent with applicable law.[7] The new service provider reporting requirement together with the Fed's efforts to improve access to service provider reports should help to streamline small banks' efforts to monitor their technology service providers.

The Federal Reserve System Focus on Cyber Risk

The financial system is deeply interconnected. As a result, the Federal Reserve coordinates with industry and a number of domestic and international agencies, governance bodies, and state and federal regulators to share information and best practices to prevent, detect, and recover from cyberattacks. These efforts enable the Federal Reserve to work closely with other regulatory agencies to issue consistent guidance and updated examination procedures on critical areas including IT risk management and cybersecurity.

Of course, a critical element of the Fed's focus on cybersecurity risk is the expectation that a bank will continue to develop internal expertise and build upon that expertise over time. Similarly, the Federal Reserve is committed to ensuring that our supervision is well positioned with appropriate staffing, training, and resources to understand and effectively examine cyber risk. We recognize that expertise in this area is critical for our success as well, and the Reserve Banks have been actively recruiting seasoned cybersecurity and IT specialists, while also working to develop in-house expertise.

Examiner training is frequently updated to align with current and emerging threats, and the Federal Reserve actively prepares examiners when new cyber risk management guidance is released. IT examiners also get industry perspective through participating in external conferences and training events from cybersecurity experts and organizations. In short, the Federal Reserve is committed to ensuring that examiners are well-positioned to supervise the efforts of state member banks and bank holding companies to address cyber-risks, and to provide more effective outreach and communication.[8]

Today's workshop is just one of the many ways we engage with banks on cyber-related issues.

Because cyber threats evolve quickly, cybersecurity must be equally dynamic in its response. Banks must continuously refine their risk management processes. We recognize the importance of regular communication and outreach through events like this one today. While we expect banks to be in touch with us when an event happens, cyber events should not be the first time a cyber-risk conversation occurs between a bank and its regulator. We look forward to working with you to assist in clarifying expectations, applying regulatory guidance or seeking feedback on cyber-risk management strategies. We encourage bank management teams to engage with regulatory points of contact whenever questions arise on cyber security matters just as with any other regulatory matter.

Closing Remarks

In closing, the pace of technological change continues to accelerate. We recognize that banks need to adopt new technologies to meet customer demands, to take advantage of efficiencies and cost savings, and to remain competitive in the marketplace. Although third-party relationships are one avenue for community banks to bring new technologies online, they must do so with a thorough understanding of the associated risks.

The Federal Reserve is committed to working together with the other regulators to continue providing guidance and resources, like this workshop, to ensure that banks are appropriately managing cyber risk.

Thank you again for the invitation be with you today. I hope this workshop demonstrates the value of open communication between bankers, regulators, industry, and law enforcement so that we may continue to work together in building resilience in the financial system to ever-evolving cyber risks.

---

[1] The views expressed in these remarks are my own and do not necessarily reflect those of my colleagues on the Board of Governors of the Federal Reserve System.

[2] See Board of Governors of the Federal Reserve System, *Cybersecurity and Financial System Resilience Report* (PDF)(Washington: Board of Governors, July 2022).

[3] See "Phishing," (PDF) Cybersecurity and Infrastructure Security Agency.

[4] See Federal Deposit Insurance Corporation, *Risk Review* (PDF) (Washington: Federal Deposit Insurance Corporation, June 2022).

[5] See Proposed Interagency Guidance on Third-Party Relationships: Risk Management, 86 Fed. Reg. 38182 (July 19, 2021).

[6] See "SR 21-15 / CA 21-11: Guide for Community Banking Organizations Conducting Due Diligence on Financial Technology Companies," Board of Governors of the Federal Reserve System, last modified September 15, 2021.

[7] See Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66424 (effective April 1, 2022).

[8] See Board of Governors of the Federal Reserve System, *Cybersecurity and Financial System*.