Perspectives on Cybersecurity, the Financial System, and the Federal Reserve

Loretta J. Mester
President and Chief Executive Officer
Federal Reserve Bank of Cleveland

2019 Ohio Bankers Day
Ohio Division of Financial Institutions
Columbus, OH

April 4, 2019

Introduction

I thank the Ohio Division of Financial Institutions for inviting me to be a part of the 2019 Ohio Bankers Day. Bankers have a unique perspective from which to gather information on the health of the economy. I appreciate the insights I gain from speaking with bankers throughout the Cleveland Fed's District, including those who serve on our Board of Directors and our Community Depository Institutions Advisory Council, and I am looking forward to hearing your questions and comments after my prepared remarks.

I do not need to tell this audience that banking plays an important role in supporting a strong economy. The credit, savings, and payment services banks provide help to foster economic growth. In offering these financial services, banks have to take on risk, and managing that risk is essential to ensuring that the financial system remains resilient. The financial crisis painfully demonstrated the high costs imposed on households, businesses, and banks – indeed, the entire economy – when the financial system is impaired.

Much progress has been made since those dark days. Regulatory changes and the steps bankers themselves have taken to shore up their risk management practices have led to a stronger and safer banking system. The banking system is better capitalized, institutions are in a stronger liquidity position, there is an effective regime for stress testing, and the ability to resolve the largest institutions when they falter has been improved. Regulators are now in the process of tailoring the regulatory regime so that the strictest requirements are imposed on those institutions that pose the largest risks and the regime can continue to support financial system resiliency.

Even though progress has been made, we should never forget that the financial system is constantly evolving and there will always be new risks on the horizon to assess and manage. Perhaps the most dynamic risks are those related to cybersecurity, which I will focus on for the majority of my talk. But before that, I would like to spend a few minutes on the economy and monetary policy. Of course, the

views I will present today are my own and not necessarily those of the Federal Reserve System or my colleagues on the Federal Open Market Committee (FOMC).

The Economy and Monetary Policy

The Federal Reserve's monetary policy goals, which are mandated by Congress, are price stability and maximum employment. Currently, with respect to these goals, the overall economy is doing well: labor markets are strong and underlying inflation is consistent with our 2 percent goal. But recent data have been mixed and indicate that growth softened in the first quarter compared to last year's 3 percent pace. In my view, the most likely case is that this weakness will be temporary and that growth for the year will be at or slightly above my estimate of 2 percent trend growth, that labor markets will continue to be strong, and that inflation will stay near 2 percent, aside from the transitory effects of changes in energy prices and the usual volatility in the monthly data.

On the positive side, incomes continue to grow, reflecting the strength of the labor market, and recent readings indicate that labor productivity is rising after being quite low over the past five years. In addition, the tightening in financial conditions in the fourth quarter of last year has mostly reversed, and business, consumer, and investor sentiment have improved since the start of the year. The postponement of additional tariffs that were set to be imposed on imports from China has reduced some uncertainty and has given firms more time to reorient their supply chains. A resolution of uncertainty around trade policy could encourage further investment spending. Our District contacts across a number of sectors report that business is good and has picked up after slowing at the end of last year. On the down side, continued uncertainty over trade policy could weigh on investment spending; growth abroad, including in Europe and China, is slowing; and the outcome of Brexit is unclear. In addition, corporate debt is at very high levels; underwriting standards on leveraged loans have been weakening for some time, with a larger share of these loans going to less creditworthy borrowers; and commercial real estate valuations remain lofty. These factors have the potential to amplify an economic downturn, were one to occur.

At its March meeting two weeks ago, the FOMC elected not to make any change in its policy rate, the federal funds rate, and I supported that decision. The current target range for the federal funds rate is 2-1/4 to 2-1/2 percent, which is at the bottom of the range of FOMC participants' estimates of its longer-run neutral rate, a level that neither stimulates nor restricts the economy and is consistent with maximum employment and price stability. Given the current level of interest rates, and little sign that inflation is poised to rise appreciably despite the strength in labor markets, I see no urgency to change our policy stance. In my view, monetary policy does not appear to be far behind or far ahead of the curve. Before determining any further adjustments in the policy rate, we can take the opportunity to continue to gather information, see how the economy is evolving, and assess our medium-run economic forecast and the risks to that forecast. Could we be done with policy rate increases this cycle? It is possible, but if the economy performs along the lines I think is the most likely case – with growth picking back up to, or slightly above, trend, labor markets remaining strong, and inflation staying near 2 percent – the fed funds rate may need to move a bit higher than current levels. As we continue to assess the outlook, I believe that the economy is going to give us a good sense of whether policy is where it needs to be or whether further action is needed.

At its March meeting, the FOMC also released further information regarding our plans for normalizing the Fed's balance sheet. Our intention is to hold no more assets than the amount necessary to implement monetary policy effectively and efficiently within an abundant reserves framework. The Fed's balance sheet grew as a result of actions we took to address the financial crisis and Great Recession. Once we had moved our policy rate down to essentially zero, to add further monetary accommodation, we began purchasing agency mortgage-backed securities, agency debt, and longer-term Treasury securities in order to put downward pressure on long-term interest rates. The assets on the Fed's balance sheet swelled, and bank reserves, one of the liabilities on our balance sheet, rose substantially. Since October 2017, the Fed has been letting these longer-term assets gradually roll off our balance sheet, and bank reserves are now down considerably from their peak level. We will be slowing the asset runoff in May and will cease the

runoff at the end of September. At that point, the average level of reserves will still likely be somewhat above the level needed to implement monetary policy efficiently and effectively. So we anticipate keeping the amount of assets on our balance sheet roughly constant for a time, and as currency and other non-reserves liabilities continue to gradually rise, reserves will gradually fall. Once the FOMC decides that reserves have declined to the necessary level, assets will begin to rise again to keep pace with the trend growth in demand for our non-reserves liabilities and to maintain the appropriate level of reserves in the system.[1] In terms of the composition of the Fed's balance-sheet assets, the FOMC plans to return to holding mainly Treasury securities and will be making decisions on how best to make that transition at upcoming meetings.

That is a brief summary of my views on the economy and monetary policy. Now let me turn to cybersecurity.

Cybersecurity Is an Important Part of Financial Stability

It would be difficult to determine the level of safety and soundness of an individual bank or of the financial system overall without paying attention to the risks to cybersecurity. While much progress has been made to address more typical banking risks, including credit, liquidity, and operational risks, cyber risks are expanding. As businesses have become more reliant on technology, efforts to disrupt an institution's operations; to steal, corrupt, or destroy data and intellectual property; or to divert funds have become more prevalent. Although it is hard to come up with firm numbers, the U.S. Council of Economic Advisers has estimated that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016, and other estimates suggest those costs are rising.[2] Firms are spending significant amounts on their cybersecurity, with one estimate at nearly $124 billion globally in

[1] Federal Open Market Committee (2019).

[2] Council of Economic Advisers (2018) and Kashyap and Wetherilt (2018).

2019.[3] While all businesses face cyber risks, given the critical role the financial sector plays in the overall health of the U.S. and global economy, the stakes are particularly high in the financial services industry.

Cyber risks could be viewed as a form of operational risk, but given the potential for the widespread impact of cyber attacks on the financial sector, I think it pays to put cyber risks into a special category.[4] One reason is that cyber risks are becoming increasingly sophisticated. Cyber attacks have become more systematic, maliciously targeting financial firms and playing out over time for maximum effect. So, increasingly creative solutions must be found to address cyber risks. One example is Sheltered Harbor, an industry initiative that provides participant financial institutions a way to store data independent of the bank's own infrastructure. This can help make recovery quicker after an attack is detected.[5] But a further complication is that detection can be difficult; an institution may believe it has backed up its good data, but those data may already have been compromised by malicious code that has infiltrated the institution's system.

Instead of being idiosyncratic and affecting only a few firms, as many operational risks are, cyber threats are more likely to be correlated across institutions because of the complex interconnections and dependencies among financial firms. This means cyber threats are more likely to have wider spread negative impacts than a typical operational problem that might arise from a failed system or process. Trading platforms, settlement and payments systems, and central securities depositories are all critical infrastructures on which financial firms depend, and if these systems go down, there are few substitutes. In addition, the advent of new technologies like cloud computing creates another concentrated risk, as there are only a handful of third-party providers of these services.

---

[3] See Kashyap and Wetherilt (2018).

[4] Kashyap and Wetherilt (2018) and Healey, et al. (2018) discuss how cybersecurity differs from other types of operational risks in the financial sector.

[5] See shelteredharbor.org for further information.

As much as individual firms are investing in cybersecurity – and it is a lot – as a nation and globally, we are likely underinvesting. This is because cybersecurity is a public good: the overall financial system conveys benefits to us all. Individual institutions certainly have incentives to invest in their own cybersecurity, and banks have been making major investments to monitor and protect their systems against attack. But the social benefit conveyed by a well-functioning and resilient financial system, one in which the public can continue to have a lot of confidence, likely requires a higher level of investment in cybersecurity than what individual firms would decide to do on their own, as they consider the tradeoff between the risk of loss to their firm from a cyber attack versus the cost of that investment. In addition, to the extent that individual firms are relying on shared services, in considering how much to invest in their own cybersecurity, they should be entertaining the possibility that those shared services could be heavily taxed in the event other firms are attacked at the same time they are [6] or that the shared service itself could be the entry point for a system-wide attack. These types of externalities may not be part of any one firm's investment decision. Moreover, an individual firm may rely on others in the shared network to make investments that make the network more secure, but if every firm thinks this way, there will be underinvestment in security.[7]

Cybersecurity and the Fed

The public good aspect of cybersecurity and the Federal Reserve's role in ensuring the resiliency of the financial system mean that cybersecurity is a high priority for the Fed. The Fed's approach builds on techniques that we have successfully applied to other forms of financial system oversight, namely, developing clear and consistent standards for assessing financial institutions' preparedness; establishing corporate governance best practices with respect to cybersecurity; acquiring and deploying Fed staff with

[6] See Kashyap and Wetherilt (2018).

[7] Sablik (2017) discusses the underinvestment problem. See, also, the Council of Economic Advisers (2018). The U.S. Department of the Treasury (2013) outlines the role government incentives can play in driving private-sector actions to strengthen defenses against cyber threats.

the necessary technical skills to assess risk-management practices; and encouraging and creating avenues for information sharing among financial institutions and regulators.

While much of the Fed's cybersecurity effort focuses on the nation's largest, most complex banking organizations, we have raised the expectations of cyber preparedness for all of the institutions we supervise, including regional and community banks. In fact, since 2015, the Cleveland Fed has been co-leading the Federal Reserve System's annual national horizontal review of cybersecurity for banks with assets between $100 billion and $500 billion. Fed examiners assess a bank's cybersecurity along a number of dimensions. Effective cybersecurity requires effective cyber-risk governance, including leadership's engagement in oversight of the firm's cybersecurity programs. The bank needs to have effective programs for identifying risks and vulnerabilities, including those within its own technology infrastructure, those associated with vendors and third-party technology providers, and those posed by new products. The bank is also assessed on its ability to monitor and manage those risks. This includes basics such as adequate technology inventories and timely software patching to more complex processes for incident response and plans for timely recovery and restoration of critical functions.

The Fed continues to work with other U.S. financial regulatory agencies and international authorities to harmonize cyber risk-management standards and regulatory expectations. We are looking for ways to coordinate cyber-risk supervisory activities for institutions subject to oversight from multiple regulators. The Fed is also aligning what it expects of banks in terms of identifying, protecting, detecting, responding to, and recovering from cyber attacks with the best-practice standards in the National Institute of Standards and Technology's (NIST) cybersecurity framework.[8]

Given the systemic nature of cyber risks and the potential for widespread disruption, collaboration between the regulators, government, financial institutions, and other private-sector firms is a crucial

[8] See Quarles (2018)

ingredient for improving our cybersecurity. One form of this collaboration is tabletop exercises, which can improve the readiness of the industry and government to respond to a cyber incident. The Fed participates in the Hamilton Series of tabletop exercises, in collaboration with the U.S. Department of the Treasury and the Financial Services Information Sharing and Analysis Center (FS–ISAC), an important banking industry forum that promotes collaboration on critical security threats. These exercises are intended to improve public- and private-sector management of cyber risks. Participants have told us that they value these exercises because they promote consistent approaches and best practices in event response and recovery, and foster relationships with key regulatory officials.

Further development and use of stress testing to assess the financial system's resilience to cyber risks would be helpful. Just as horizontal stress testing has proven to be a useful tool in assessing the overall resilience of the financial system to credit and liquidity risks, stress testing could be used to assess how prepared individual firms and the overall system are to respond to and recover from a systemic cyber event such as the shutdown of a major clearing or settlement bank. Such a test could help evaluate firms' plans for data and core systems recovery and their reliance on third parties to implement that plan. The Bank of England is applying these stress-testing techniques to evaluate whether financial firms are able to resume services within the tolerance set by the Bank of England in the face of a system-wide attack or data corruption that affects multiple firms and their service providers.[9]

Because cyber threats are not restricted by national borders, cross-border collaboration is also being pursued. For example, in November 2015, the U.S. and U.K. governments conducted a joint exercise with leading global financial firms to determine how the two governments would perform in the event of a large cyber attack on the financial systems in both countries.[10] The Fed participated in the exercise, which evaluated incident-response handling and recovery, coordination, public communication, and

[9] See Kashyap and Wetherilt (2018).

[10] See U.S. Department of the Treasury (2015).

information handling.

Indeed, information sharing is another critical ingredient for improving our cybersecurity. Without firms' willingness to share information on cyber incidents, it is much harder to develop metrics to evaluate cyber resilience, to assess whether threat levels are rising or beginning to propagate through the financial system, and to determine whether the practices firms have in place actually are working to mitigate the risks. The Fed has been working with FS-ISAC to promote information sharing, and the Cleveland Fed is playing a national role in the collection of threat information. The Fed's Cybersecurity Analytic Support Team (CAST) was created in 2015 and is based at the Cleveland Fed. This team tracks the latest cybersecurity developments across the financial sector in critical payment, clearing, and settlement systems, allowing it to gain a wide perspective on potential threats to the overall financial system and to better calibrate threat severity and impact. As its name implies, CAST casts a wide net in collecting this information and collaborates with the U.S. Department of the Treasury, other bank regulatory agencies, and the FBI. In addition to Federal Reserve System-level activities, the Cleveland Fed staff is also sharing its expertise on cybersecurity topics at industry and regulatory forums, and last year, the staff organized a regional conference on managing cyber risks from the C-suite, which some of you attended.[11]

Finally, the Federal Reserve is a provider of both wholesale and retail payment services to the public and the U.S. government. We need to maintain the public's trust and confidence in our ability to deliver those services, so we are highly engaged in work to enhance the resiliency of our own systems, applications, and data against cybersecurity risks. We continue to be pro-active in looking for emerging threats and testing our systems and processes for vulnerabilities.

This is only a brief summary of the work that is being done at the Federal Reserve, in partnership with other financial regulators, government agencies, and financial institutions, to help address the cyber risks

[11] More information on the Cleveland Fed's work on cybersecurity is available on our website at clevelandfed.org. See, for example, Stone (2018), which discusses key cybersecurity risks and implications for the financial sector and consumers.

to our financial system. The work includes enhancing systems for detecting and monitoring cyber risks, as well as improving our collective ability to respond to and recover from an attack. The landscape is very dynamic. New cyber risks are emerging; they are becoming more sophisticated and complex. Given the importance of the financial system to our economic health, it is incumbent on us all to continue to work together with some urgency so that we are better prepared for cyber threats to our financial stability.

References

Council of Economic Advisers, "The Cost of Malicious Cyber Activity to the U.S. Economy," February 2018.
(https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf)

Federal Open Market Committee (FOMC), "Balance Sheet Normalization Principles and Plans," March 20, 2019.
(https://www.federalreserve.gov/monetarypolicy/policy-normalization.htm)

Healey, Jason, Patricia Mosser, Katheryn Rosen, and Adriana Tache, "The Future of Financial Stability and Cyber Risk," The Brookings Institution Cybersecurity Project, October 2018.
(https://www.brookings.edu/research/the-future-of-financial-stability-and-cyber-risk/)

Kashyap, Anil K., and Anne Wetherilt, "Some Principles for Regulating Cyber Risk," Centre for Economic Policy Research (CEPR) Discussion Paper No. DP 13324, November 17, 2018, and *American Economic Review Papers and Proceedings*, forthcoming.
(http://faculty.chicagobooth.edu/anil.kashyap/research/papers/Some_Principles_for_Regulating_Cyber_Risk.pdf)

Quarles, Randal K., "Brief Thoughts on the Financial Regulatory System and Cybersecurity," at the Financial Services Roundtable 2018 Spring Conference, Washington, D.C, February 26, 2018.
(https://www.federalreserve.gov/newsevents/speech/quarles20180226b.htm)

Sablik, Tim, "Cyberattacks and the Digital Dilemma," Econ Focus, Federal Reserve Bank of Richmond, Third Quarter 2017.
(https://www.richmondfed.org/-/media/richmondfedorg/publications/research/econ_focus/2017/q3/cover_story.pdf)

Stone, Sydney, "The Threats, the Criminals, the Motives – Cybersecurity at the Fed," Federal Reserve Bank of Cleveland, November 26, 2018.
(https://www.clevelandfed.org/newsroom-and-events/multimedia-storytelling/cybersecurity.aspx)

U.S. Department of the Treasury, "Treasury Department Report to the President on Cybersecurity Incentives Pursuant to Executive Order 13636," 2013.
(https://www.treasury.gov/press-center/Documents/Supporting%20Analysis%20Treasury%20Report%20to%20the%20President%20on%20Cybersecurity%20Incentives_FINAL.pdf)

U.S. Department of the Treasury, "Joint Statement from the U.S. Department of the Treasury and Her Majesty's Treasury," November 12, 2015.
(https://www.treasury.gov/press-center/press-releases/pages/jl0262.aspx)