Kevin Stiroh: Introductory remarks at the Community Bankers Conference

Remarks by Mr Kevin Stiroh, Executive Vice President of the Financial Institution Supervision Group of the Federal Reserve Bank of New York, at the Community Bankers Conference, Federal Reserve Bank of New York, New York City, 18 April 2018.

* * *

On behalf of the Federal Reserve Bank of New York, it's my pleasure to welcome you to the 2018 Community Bankers Conference. This is the third Community Bankers Conference that I've attended since becoming the head of Supervision at the New York Fed and it is great to see the turnout continue to grow. This year we are fortunate to have nearly one hundred fifty representatives from community banks throughout the Federal Reserve's Second District and more than forty regulatory colleagues from multiple federal and state agencies.

Each year I look forward to this conference as it offers us, as regulators and supervisors, an unparalleled opportunity to exchange views and perspectives, to identify challenges and opportunities, and to promote a robust dialogue with senior managers and directors of smaller financial institutions in the Second District. This type of constructive engagement is critical for us as we work to promote a safe and sound financial system that supports a strong economy.

The theme of this year's conference—"Navigating Future Risks for Community Banks"—is centered on *change*, which is appropriate when one considers the broad set of forces transforming the U.S. financial system. As you all know, the banking industry is confronting a series of emerging challenges and environmental changes such as a rising interest rate environment, new businesses and technologies that may disrupt the traditional financial services industry, and novel cyber-threats that seek to exploit our highly interconnected society. In addition, over the past year or so, we've witnessed significant turnover in the leadership at federal regulatory bodies including the Federal Reserve, the FDIC, and the OCC, which has the potential to change the regulatory environment. And, finally on the legislative front, Congress is currently considering the Economic Growth, Regulatory Relief, and Consumer Protection Act, which if passed in current form would entail the most significant statutory change to the U.S. banking regulatory framework since the passage of the Dodd-Frank Act in 2010. All of this change presents both opportunities and threats.

For my remarks today, I'd like to explore three specific changes that are relevant for community banks: first, a shift in community banks' business models in response to market changes and regulatory pressures; second, the growing competition and potential disruption introduced by "fintech" firms; and third, the critical threat that cybersecurity risks pose to all community banks. Following my remarks and throughout the day, I look forward to hearing from you about these forces as well as on other changes, trends, and challenges that you and your firms are facing.

Before I begin, I'd like to thank the organizers of this conference for putting together today's informative and timely program, as well as our many speakers and panelists for their participation. In addition, please note that my comments today are my own and do not necessarily represent those of the Federal Reserve Bank of New York or the Federal Reserve System.

Community Bank Business Models: Recent Trends

I'll begin with some observations on recent trends in community bank lending. This perspective is critical because, as New York Fed President Bill Dudley stated in his welcoming remarks, community banks are a vital component of the U.S. banking system. They provide an array of financial services to a wide range of customers and business sectors. This is particularly

important as many of these sectors are considered “underserved” due to the limited presence of physical banking locations in their locales.

As background, the New York Fed is the primary supervisor for 17 community banks and over 100 bank holding companies that operate throughout Upstate New York, in parts of Connecticut and New Jersey, and in the greater New York City area. Our staff in supervision monitors trends and emerging risks in the financial services industry across the Second District, including those associated with community banks. These analyses along with insights we gain directly from interaction with community bankers inform our supervisory programs and allow us to tailor our examination strategy and risk-focus for community banks.

I’ll highlight a few interesting trends that our examiners and analysts have observed through this monitoring. For the three-year period ended December 31, 2016, aggregate Second District community bank loans grew by 46 percent.[1] These loans were often funded by non-core funding sources, which grew by 49 percent in the aggregate over the same period. This raised concerns among supervisors who consider non-core funding sources as higher risk from a safety and soundness perspective.

Moreover, the primary source of loan growth for this period was commercial real estate. In response to this growing CRE concentration, the Fed intensified its monitoring of this sector and directed our supervisory focus toward how firms are risk-managing their CRE portfolios.

More recently, during 2017, we saw more moderate asset growth for community banking organizations in the District—approximately 7.5 percent—which is in line with national peer group averages. Aggregate loan growth in 2017 was 10.5 percent for the year, which is also comparable to the national peer group averages. Over this period, we observed a small shift from commercial loan growth toward retail loan growth, specifically in the areas of one-to-four family homes and indirect automobile loans. With respect to funding in 2017, we observed strong growth in core deposits and less reliance on non-core funding sources—a positive trend from a safety and soundness perspective.

In the competitive environment of the Second District, we’ve observed community banks seeking revenue from more niche businesses such as wealth management and indirect automobile lending. We’ve also observed community banks participating with other banks on real estate lending, in part to better manage real estate concentrations. Community banks are also seeking to differentiate themselves from their larger competitors by marketing their more individualized customer service.

In regard to liquidity, a number of community bankers have noted the influx in public deposits and the challenges associated with putting these deposits to productive use.

Finally, although there has been a material improvement in asset quality over the last several years, it will be important for senior management to continue to be prudent in their underwriting practices and in monitoring any emerging risks in their portfolios. The economy continues to show a strong trajectory, but of course we need to remain alert to any potential slowdown.

As Second District community banks grow in line with their national peers, we are encouraged by the increased reliance on core funding and strong asset quality. We will, however, continue to monitor developments that may pose a risk to the safety and soundness of the financial and banking system.

Fintech

A second major change for community banks—like all banking institutions—is the potential competition from new “fintech” firms. Since 2012 there has been over $40 billion in US-based fintech investments including online lending-based platforms, capital markets, and payment and

settlement services.[2] By offering traditional financial services to customers through new, innovative platforms and channels, these fintech firms pose a challenge to traditional banking business models.

Many community bankers are taking a proactive, forward-leaning approach to these new technologies with a focus on how they can be leveraged to improve their business and benefit their customers. Among the opportunities community bankers have highlighted during our discussions are: technological solutions that reduce back office costs; more efficient loan processing; and an improved customer experience through smartphone applications and other mobile technology. This proactive perspective leverages innovation as a strategic differentiator and competitive advantage, rather than just a means to enhance efficiency.

The speed and magnitude of these changes also have implications for us as supervisors. We must keep pace and understand the risks associated with innovation so that we can appropriately focus our supervisory efforts on new operational, compliance, and reputational risks. For example, Supervisory and Regulatory Letter 13–19, "Guidance on Managing Outsourcing Risk," provides supervisory expectations on partnering with outside vendors. While supervisors can provide some focus on emerging risks, it is ultimately the responsibility of each firm and its board to identify the relevant risks associated with new technologies and make appropriate and prudent business decisions for their institutions and customers.

Cybersecurity

The potential benefits associated with these new technologies are accompanied by the risks posed by cybersecurity. Cybersecurity risks, the third topic on my list, continue to raise challenges for all types of firms in the financial system, ranging from supervised banks to financial utilities to non-bank financial firms to government agencies. While these entities differ in size, purpose, and mission, the common threats associated with cybersecurity represent a universal concern. Indeed, in my regular meetings with supervisory colleagues and supervised institutions, cybersecurity is almost always at the top of the risk list. Frequently cited challenges by local institutions include: attracting and retaining information technology talent, as these skilled individuals are in high demand and implementing a sufficiently robust vendor management program for technology services outsourced to third-party providers.

While we expect firms to adequately manage a number of financial and operational risks such as credit risk, market risk, and operational risk, the nature of the cybersecurity risk differs in one key aspect – motivation. A cybersecurity attacker might be a nation-state or hacker with the intention to disrupt or damage a critical infrastructure sustaining the U.S. and global economy. Or, the attack may be financial in nature, where the perpetrator is engaging in fraud and seeking to profit. These motivations suggest that the cyber threat is more intentional than other risks. This intentionality coupled with the resources of some perpetrators raises the stakes significantly and makes cyber defense much more difficult.

We recognize that addressing the cyber threat is a complicated and expensive undertaking, but it is an essential one. All banks, from the largest globally systemically important to the small community banks, are vulnerable to this threat and need to take the appropriate steps to identify, protect, detect, respond, and recover.

A critical aspect of cybersecurity is the need for banks to adequately invest in safeguarding their systems and platforms by training their employees on how to identify potential cyber-attacks, mitigate vulnerabilities, and escalate issues appropriately. Moreover, to address potential insider threats, banks must establish and maintain robust protocols and controls in managing employees' access to the firm's systems and databases. Ensuring that sensitive firm data, personal information, and critical infrastructure are accessible only to those trusted employees who need access is vital to guard against accidental or intentional data loss, theft, or damage.

Supervisors expect that institutions create a strong risk culture around access control and vendor management. Employees are banks' first lines of defense against cyber vulnerabilities, so investment in employee training is critical. By raising awareness about potential threats and vulnerabilities, a bank can equip employees with the knowledge and judgment to recognize attacks such as social engineering and mitigate the impact. In addition, training can reduce the probability that an employee will unintentionally cause a breach. For example, we have seen deficiencies due to weak internal controls and policies and procedures, which have led to increased exposure to cybersecurity risk. Institutions are expected to ensure service providers comply with applicable regulations that are consistent with safe and sound banking practices.

Closing

I've outlined three major, transformative changes and trends that all of us in this room—community bankers, regulators, and supervisors—are currently facing. During the panels, formal Q&As, and sidelines of the conference, I encourage you to share your views on these topics and other changes that you are confronting, with a focus on the opportunities, risks, and mitigants.

By sharing our perspectives, community banks can continue to play a central role in the sustainable provision of financial services to customers in the Second District. Moreover, by working together to address these changes, the New York Fed and the broader regulatory community will be better positioned to achieve its goal of creating safe, sound, and stable banking and financial systems that support the U.S. economy.

Thank you for your attention.

---

1 Aggregate Second District data is based on Call reports and UBPR data from 114 firms.

2 Fintech Trends to Watch in 2018, CB Insights.