FEDERAL RESERVE SYSTEM

COMMUNITY BANKING
CONNECTIONS®

A SUPERVISION AND REGULATION PUBLICATION

A Message from Governor Bowman

by Governor Michelle W. Bowman

Third Issue 2021

Governor Michelle W. Bowman

Members of the *Community Banking Connections* Advisory Board interviewed Governor Michelle W. Bowman for her insights on the Federal Reserve's efforts to address the challenges and risks faced by community banks.

You've highlighted the importance of outreach with community bankers and how these conversations help shape your supervisory policy priorities. Can you provide examples of how your outreach discussions have influenced the Federal Reserve's policies and supervisory process?

Two recent examples highlight how my conversations with community bankers have resulted in tangible outcomes that have addressed challenges identified by community banks.

The first example is the current expected credit losses (CECL) methodology. A number of conversations with community bankers included a discussion of concerns about the complexity and cost of implementing CECL. To address these concerns, I encouraged Federal Reserve staff to look for ways to ease the burden of CECL implementation for community banks.

During a July 15, 2021, Ask the Fed webinar, Fed staff and I introduced the Federal Reserve's Scaled CECL Allowance for Losses Estimator, which is referred to as the "SCALE" method. The SCALE method is a simple spreadsheet-based approach for CECL compliance developed to assist community banks with less than $1 billion in assets. The SCALE method is one of many acceptable CECL methods used to estimate allowances for credit losses. Just as with the other acceptable CECL methods, bank management must determine whether the SCALE method is appropriate for the bank. Additionally, Federal Reserve staff developed a customizable and semiautomated SCALE tool for community banks with total assets of less than $1 billion. If a bank chooses to use the SCALE method, the bank may access this tool at no cost. SCALE information and resources, including a recording of the webinar and a link to the tool with instructions, are available at www.supervisionoutreach.org/cecl/scale.

Second, recognizing certain challenges associated with how community banks pursue technological innovation, we made great strides on three related efforts.

On August 27, 2021, the Federal Reserve and the other federal banking agencies released an interagency vendor due diligence guide that can be used by community banks in performing due diligence on prospective and existing relationships with fintech firms.[1] The guide focuses on six key due diligence topics and includes relevant considerations, potential sources of information, and illustrative examples. Community banks can tailor their use of the guide based on specific circumstances and risks.

On September 9, 2021, the Federal Reserve released an innovation partnership paper that describes key considerations for partnering with a fintech firm.[2] This paper does not establish new supervisory expectations; it provides an overview of the evolving landscape of community bank partnerships with fintech firms and describes effective practices and considerations for seeking out and engaging in such partnerships to access new technology.

On July 13, 2021, the federal banking agencies requested public comment on proposed guidance designed to help all banking organizations (regardless of asset size) manage risks associated with third-party relationships, including relationships with fintech providers.[3] The proposed guidance should assist banking organizations in identifying and addressing the risks associated with third-party relationships and responds to industry feedback requesting agency alignment with respect to third-party risk management guidance.

The Federal Reserve made changes to its examination posture early in the pandemic. Can you share how the Federal Reserve has modified its supervisory posture to address lessons learned during the past 18 months?

On August 19, 2021, Federal Reserve staff held an Ask the Fed webinar to provide an overview of the measures taken to refine our community bank supervisory program. This webinar is archived and available at https://bsr.stlouisfed.org/askthefed/Home/ArchiveCall/309. I expect that bankers will be pleased to see that we have revitalized our supervisory approach to incorporate supervisory lessons learned during the pandemic.

In September, the Federal Reserve began transitioning away from our pandemic posture to return to a more traditional supervisory approach.[4] Since the effects of the pandemic are still present in some areas of the country, examination staff will work with states and supervised institutions to determine when onsite exams can and should resume. We will consider local health and safety conditions when making these decisions.

Some of the important lessons learned during the pandemic will influence our examination processes going forward. For example, we have refined processes for determining the scope of supervisory activities and information we request for examinations — both are highly risk focused and should minimize the examination burden on a bank. Examiners will continue to emphasize the importance of capital preservation and liquidity resiliency. Our supervisory activities will continue to focus on a bank's higher credit risk exposures and lending activities. Examiners will rely on existing guidance in conducting asset quality reviews and assigning loan classifications. However, examiners may need to engage in more in-depth discussions with bank management about a particular borrower's performance, evolving conditions, and the basis and reasonableness of cash flow projections.

I encourage you to reach out to your Reserve Bank point of contact for additional information on supervisory activities at your bank.

[1] See the August 27, 2021, press release, available at www.federalreserve.gov/newsevents/pressreleases/bcreg20210827a.htm.

[2] The paper is available at www.federalreserve.gov/newsevents/pressreleases/bcreg20210909a.htm.

[3] See the July 13, 2021, press release, available at www.federalreserve.gov/newsevents/pressreleases/bcreg20210713a.htm.

[4] In March 2020, the Federal Reserve paused examinations at smaller banks. In June 2020, the Federal Reserve resumed examination activity offsite, focusing on assessing a bank management's response to the crisis and promoting financial resiliency.

The pandemic has demonstrated the importance of technology in the examination process and the need to be able to conduct community banking organization examinations remotely. However, many community bankers have expressed the need for some face-to-face interactions with examiners. Do you envision a future in which examinations are conducted entirely offsite?

The Federal Reserve has long conducted certain supervisory activities offsite, including examination planning, scoping, and loan review. As a result, when the pandemic limited our ability to be onsite, examiners and bankers were able to quickly adapt and work remotely. However, the pandemic also limited examiners' ability to have in-person meetings with community bankers. Examiners and bankers have relied increasingly on emails, conference calls, and video technology to conduct examinations and discuss supervisory findings. In my conversations with community bankers, many have noted the value of in-person meetings with examiners.

Reflecting on the lessons learned during the pandemic, some onsite examination presence is preferred and necessary to ensure that transparent conversations between bankers and examiners continue. Further, with the pace of innovation in technology, I expect that future examinations will rely upon a hybrid approach, with some activities conducted offsite and those activities benefiting from in-person contact conducted onsite.

It's important to get the balance right, and feedback from community bankers will continue to be an important consideration when determining the appropriate ratio of on- and offsite activities. We will also need to consider a bank's ability to support offsite supervision and our ability to ensure effective and transparent communications with a community bank's board of directors and senior management.

Given your role on the Federal Open Market Committee (FOMC) what do you see as the biggest economic challenges and opportunities for community banks emerging from the pandemic?

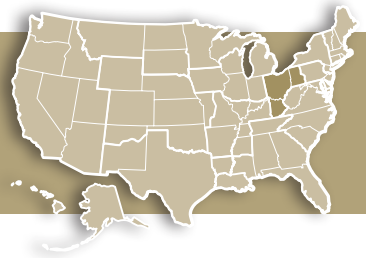
The U.S. economy is experiencing a strong rebound following last year's severe pandemic-related disruptions to employment and spending. This activity reflects not

Continued on page 28

Community Banking Connections is distributed to institutions supervised by the Federal Reserve System. Current and past issues of *Community Banking Connections* are available at www.communitybankingconnections.org or www.cbcfrs.org. Suggestions, comments, and requests for back issues are welcome in writing (editor@communitybankingconnections.org) or by telephone at 800-372-0248.

Editor: **Hilda Guay** Assistant Editor: **Maura Fernbacher**
Project Manager: **Ivy Washington** Designer: **Monica Conrad** Web Architect: **James Terry IV**

Advisory Board: **Andrea Bellucci**, Director, Examinations, Banking Supervision, FRB Dallas, **Virginia Gibbs**, Lead Financial Institution and Policy Analyst, Supervision Group, Division of Supervision and Regulation, Board of Governors, **Carolyn Healy**, Assistant Vice President, Supervision and Regulation, FRB Atlanta, **Brandon Howell**, Lead Financial Institution and Policy Analyst, Supervision Group, Division of Supervision and Regulation, Board of Governors, **Allison Lamb**, Manager, Supervision Group, Division of Supervision and Regulation, Board of Governors, **Jeff Legette**, Assistant Vice President, Supervision and Risk Management, FRB Kansas City, **Mary Luvisi**, Exam Manager 2, Supervision, Regulation, and Credit, FRB Boston, **Mark Medrano**, Assistant Vice President, Supervision and Regulation, FRB Chicago, **Mike Milchanowski**, Assistant Vice President, Supervision and Regulation, FRB St. Louis, **Shalan Miller**, Banking Supervisor, Supervision and Regulation, FRB Cleveland, **J.M. Nemish**, Senior Examiner, Supervision, Regulation, and Credit, FRB Richmond, **Natalie Richter**, Supervision Manager – CBO, Community Banks, FRB New York, **Sandra Schumacher**, Central Point of Contact/Senior Examiner, Supervision, Regulation, and Credit, FRB Minneapolis, **Joseph Sciacca**, Central Point of Contact II, Financial Institution Supervision and Credit, FRB San Francisco, **Lauren Ware**, Assistant Vice President, Supervision, Regulation, and Credit, FRB Richmond



Serving Small Businesses in a Crisis: The Role of Community Banks During the COVID-19 Pandemic

by Steve Jenkins, Senior Vice President, Supervision & Regulation, Credit Risk Management & Statistics, Federal Reserve Bank of Cleveland

Steve Jenkins

The COVID-19 pandemic continues to have unprecedented effects on economic activity around the world. In attempts to curb the spread of the disease, many state and local governments imposed stay-at-home or shelter-in-place orders that continue to impact the operations and viability of small businesses around the country. Estimates based on the Census Bureau's Current Population Survey (CPS) indicate that the number of active business owners in the United States plummeted from 15.0 million in February 2020 to 11.7 million in April 2020 and only partially rebounded by June 2020.[1] Moreover, a JPMorgan Chase & Co. survey of 2,500 small business owners found that these businesses, on average, saw their sales drop 29 percent over the second and third quarters of 2020.[2]

The Federal Reserve Bank of Cleveland has played a leading role in understanding the needs of small businesses and connecting small businesses to resources through its FedTalk series[3] and COVID-19 web page[4] and has conducted interviews to inform small businesses of loan facilities such as the Main Street Lending Program. In this article, we examine the financial challenges that COVID-19 imposed on small businesses and the role that community banks have played in helping businesses respond to those challenges through the lens of the Federal Reserve's Small Business Credit Survey (SBCS).[5]

About the Small Business Credit Survey

The SBCS is an annual survey of firms with fewer than 500 employees. These types of firms represent 99.8 percent of all employer establishments in the United States.[6] Survey respondents are asked to report information about their business performance, financing needs and choices, and borrowing experiences. The latest survey was fielded in September and October of 2020, approximately six months after the onset of the pandemic, and the results were published in February 2021. We surveyed more than 15,000 small businesses and gained key insights into how small businesses were impacted by and responded to the pandemic, including financing decisions and challenges. Data are reported by race and ethnicity of the business owner, business size, industry, and financial institution type, allowing for more granular insights into affected business segments and financial institution responses.

[1] R. Fairlie, "The Impact of COVID-19 on Small Business Owners: Evidence from the First Three Months After Widespread Social-Distancing Restrictions," *Journal of Economics and Management Strategy*, 29(4) (2020), pp. 727–740.

[2] D. Farrell, C. Wheat, and C. Mac, *Small Business Financial Outcomes During the Onset of COVID-19*, JPMorgan Chase & Co., Institute Report, June 2020, available at www.jpmorganchase.com/institute/research/small-business/small-business-financial-outcomes-during-the-onset-of-covid-19.

[3] The series is available at www.clevelandfed.org/newsroom-and-events/events/fedtalk.aspx.

[4] The web page is available at www.clevelandfed.org/en/newsroom-and-events/covid-19.aspx.

[5] C. K. Mills, J. Battisto, M. de Zeeuw, S. Lieberman, and A. M. Wiersch, *Small Business Credit Survey: 2021 Report on Employer Firms*, Federal Reserve Banks, 2021, available at www.fedsmallbusiness.org/medialibrary/FedSmallBusiness/files/2021/2021-sbcs-employer-firms-report.

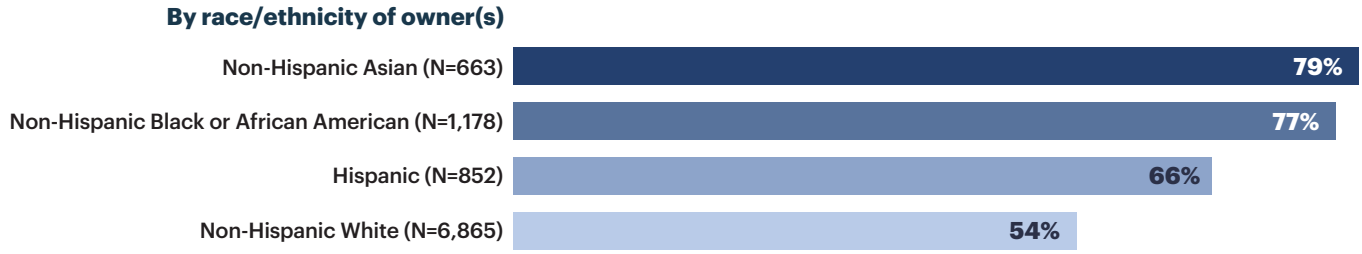
[6] Mills et al., *Small Business Credit Survey: 2021 Report on Employer Firms*.

Figure 1: Financial Condition, at Time of Survey (% of employer firms)

Note: Percentages may not sum to 100 due to rounding.

Source: *Small Business Credit Survey: 2021 Report on Employer Firms*

Figure 2: Share of Firms in Fair or Poor Financial Condition, at Time of Survey (% of employer firms)



Notes: The characteristics shown in darker bars are related to self-reported financial condition at a significance level of 0.05 using a logistic regression. The reference group is non-Hispanic White–owned firms.

Source: *Small Business Credit Survey: 2021 Report on Employer Firms*

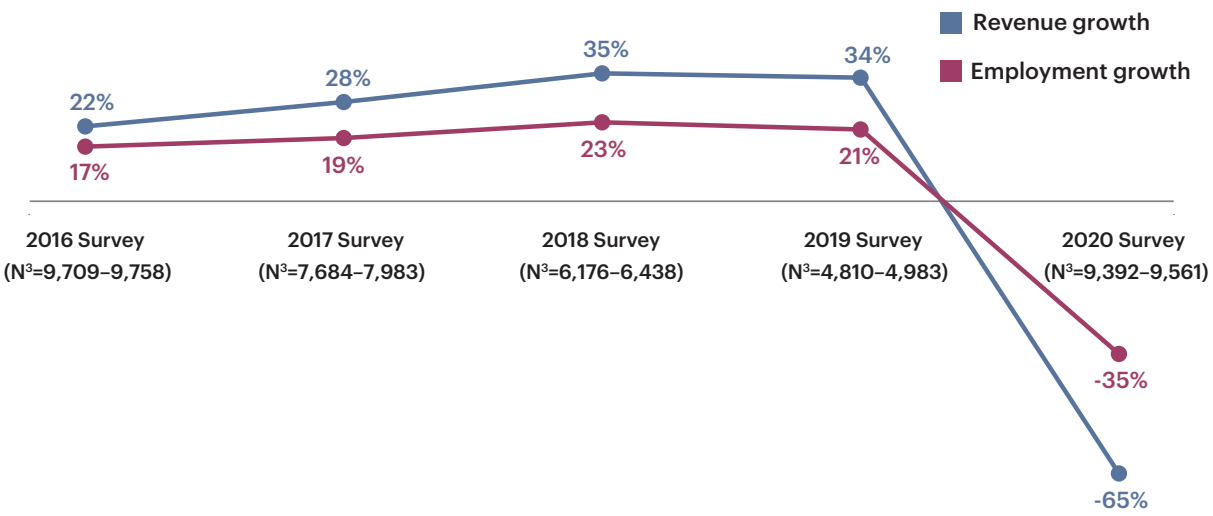
COVID-19 and Small Businesses

Not surprisingly, small businesses were hit hard during 2020. Of the SBCS respondents, 57 percent reported that their financial condition was fair or poor (see Figure 1). That percentage is even higher for minority small business owners (see Figure 2), with 79 percent, 77 percent, and 66 percent of non-Hispanic Asian, non-Hispanic Black or African American, and Hispanic business owners, respectively, reporting that their firms' financial condition was either fair or poor at the time of the survey.

Small businesses suffered deep declines in revenues and many firms reduced the number of employees. According to the survey, 13 percent of the firms reported a revenue increase in 2020, and 78 percent a revenue decline; 11 percent reported an employment increase, and 46 percent an employment decline. For the first time in five years, more firms expected revenue and employment to decline, rather than increase (see Figure 3).

Moreover, of the respondents, 81 percent reported a sales decline due to the pandemic, and approximately 53 percent said their full-year 2020 sales would be reduced by more than 25 percent because of the effects of the pandemic. These challenges are not necessarily expected to be short-lived. Seventy percent of the SBCS

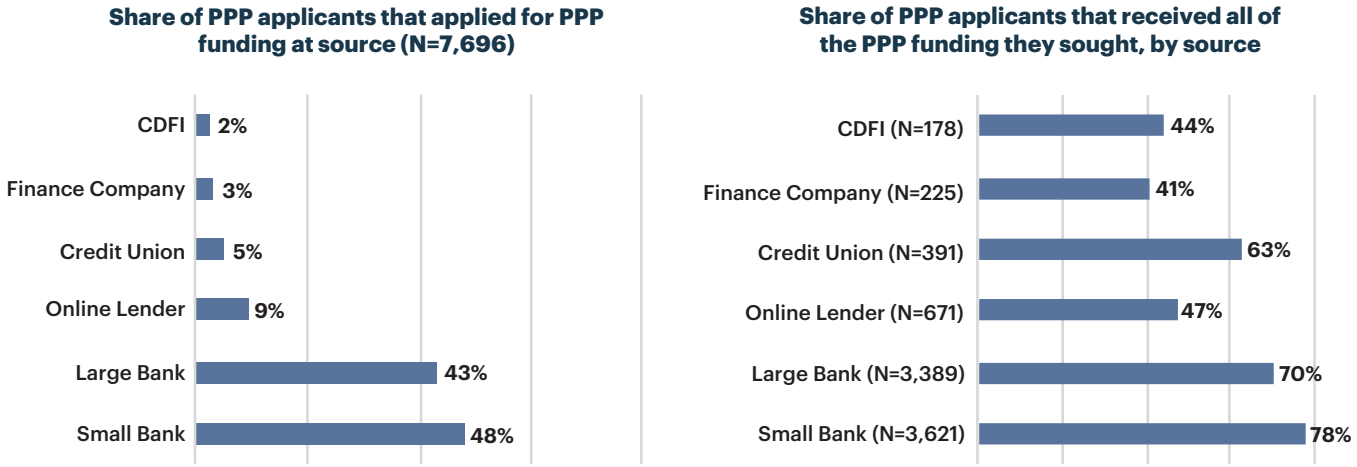
Figure 3: Employer Firm Performance Index, Prior 12 Months



Notes: The index is the share of employer firms reporting growth minus the share reporting a reduction. The 12-month period is approximately the second half of the prior year through the second half of the surveyed year.

Source: *Small Business Credit Survey: 2021 Report on Employer Firms*

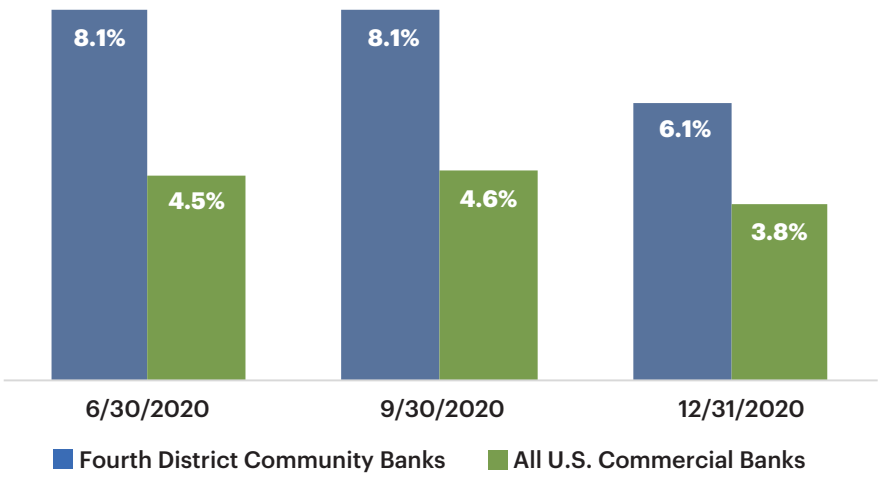
Figure 4: Paycheck Protection Program (PPP) Applications and Outcomes, by Source



Note: Respondents could select multiple options; respondents may have submitted more than one application.

Source: *Small Business Credit Survey: 2021 Report on Employer Firms*

Figure 5: PPP Loans as a Percent of Total Loans



Source: Consolidated Reports of Condition and Income (Call Reports)

respondents said it would be mid-2021 or beyond when their firms' sales returned to 2019 levels, and 30 percent of the firms experiencing below-normal sales said their businesses were either "very unlikely" or "somewhat unlikely" to survive without government assistance until their sales recover.

The challenges facing small businesses throughout the pandemic also had spillover effects on the personal finances of 80 percent of small business owners. Sixty-three percent of business owners reported that they went without a salary, while 51 percent reported that they put personal funds into the business. Given the disparate impact of the pandemic on minority businesses reflected in the survey results, the pandemic likely has had a similarly disparate impact on minority small business owner households.

The Community Bank Response

Community banks played a critical role in helping small businesses weather the first six months of the pandemic. According to the survey, 82 percent of small businesses applied for emergency funding through the Small Business Administration's Paycheck Protection Program (PPP), and community banks were critical in processing and originating those loans. While small banks[7] hold only 14 percent of commercial banking sector assets,[8] they received the largest portion of total PPP applications, 48 percent, followed by larger commercial banks[9] with 43 percent, and online lenders with 9 percent. Community banks also experienced the highest application approval rates, as 78 percent of small bank PPP applicants received all of their requested funding (see Figure 4).

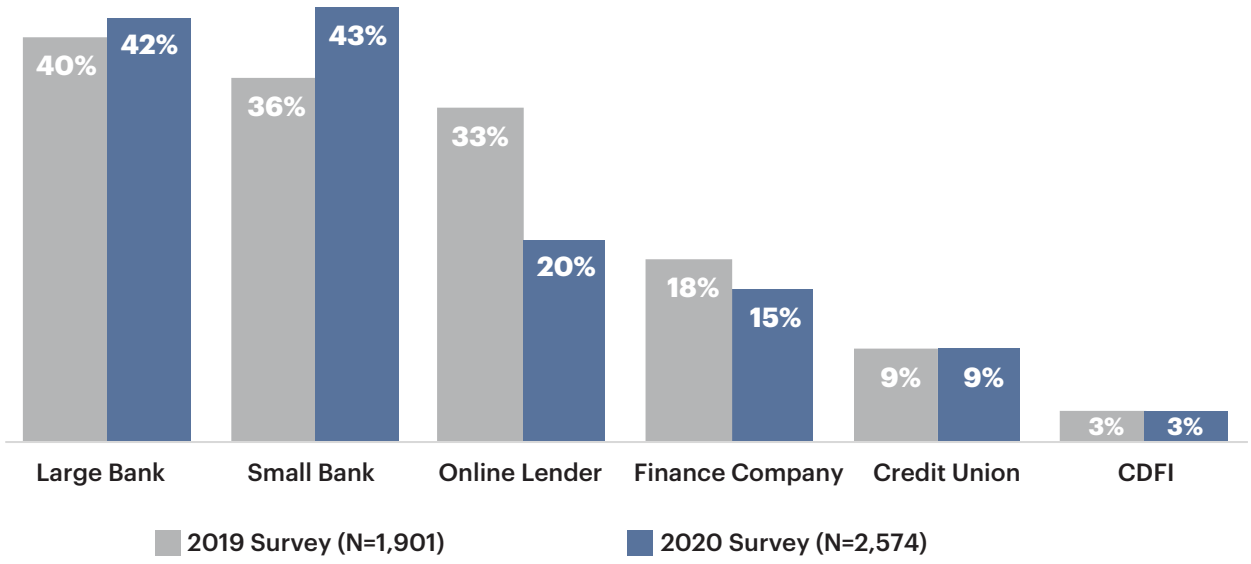
Fourth District community banks were particularly active in supporting the emergency funding needs of small businesses. As shown in Figure 5, PPP loans accounted for roughly 8 percent of the total loans at Fourth District community banks as of June 30, 2020, compared with 4.5 percent of the total loans at commercial banks nationally. By providing this vital support to small businesses, community banks may ultimately increase their small business lending market share, as anecdotal reports indicate that providing emergency funding

[7] Small banks are defined as banks with less than $10 billion in total assets.

[8] The percentage is according to Consolidated Reports of Condition and Income (Call Reports) as of December 31, 2020.

[9] Larger commercial banks are defined as banks with greater than $10 billion in total assets.

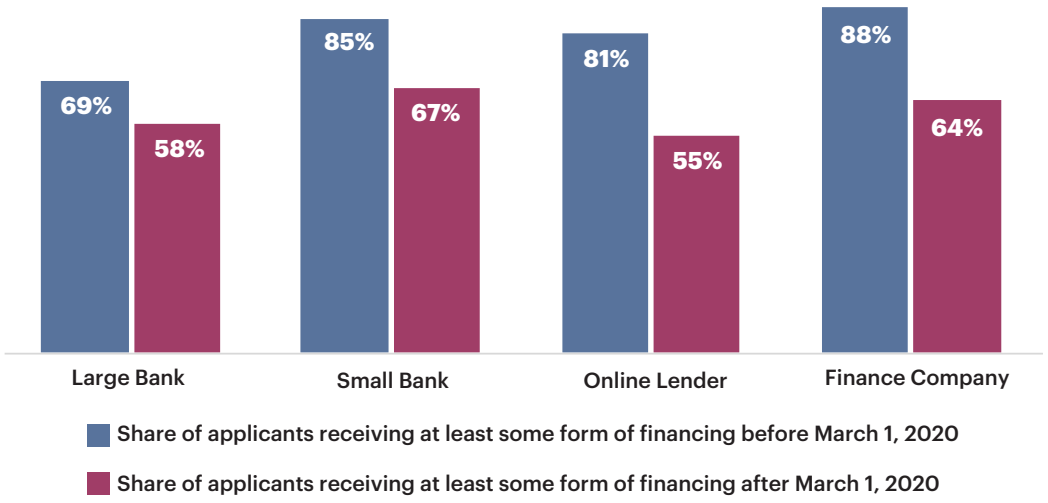
Figure 6: Credit Sources Applied to (% of loan, line of credit, and cash advance applicants)



Notes: Respondents could select multiple options; excludes emergency funding applications.

Source: *Small Business Credit Survey: 2021 Report on Employer Firms*

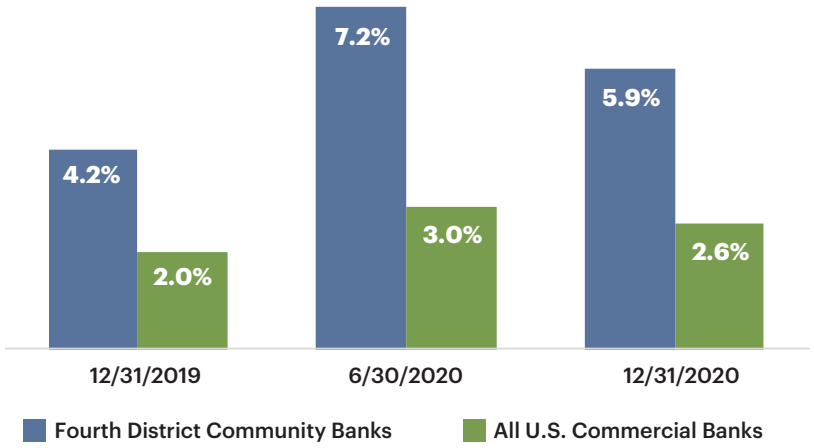
Figure 7: Approval Rates for Loan, Line of Credit, and Merchant Cash Advance Applications, by Source



Note: Approval rate is the share of approval for at least some credit.

Source: *Small Business Credit Survey: 2021 Report on Employer Firms*

Figure 8: Small Business Loans as a Percent of Total Assets



Note: Small business loans are defined as commercial and industrial loans less than $1 million.

Source: Consolidated Reports of Condition and Income (Call Reports)

support to noncustomers may translate into new permanent lending relationships.[10]

In addition to processing and originating PPP loans, community banks played a critical role in providing other sources of small business credit. According to the survey, small business customers were most likely to apply for a loan, line of credit, or cash advance through a community bank in 2020, a shift from 2019, when small businesses were most likely to apply to large banks for this funding (see Figure 6).

Community banks responded with relatively high approval rates on small business applications. As shown in Figure 7, while post-pandemic loan approval rates were below pre-pandemic levels across all financial institutions, community banks exhibited the highest small business loan, line of credit, and cash advance approval rate among financial institutions tracked in the survey.

[10] See Susan Orr, "Banks Use PPP Loans to Find New Customers, Offer Other Services," *Indianapolis Business Journal*, April 30, 2021, available at www.ibj.com/articles/alluring-appetizer.

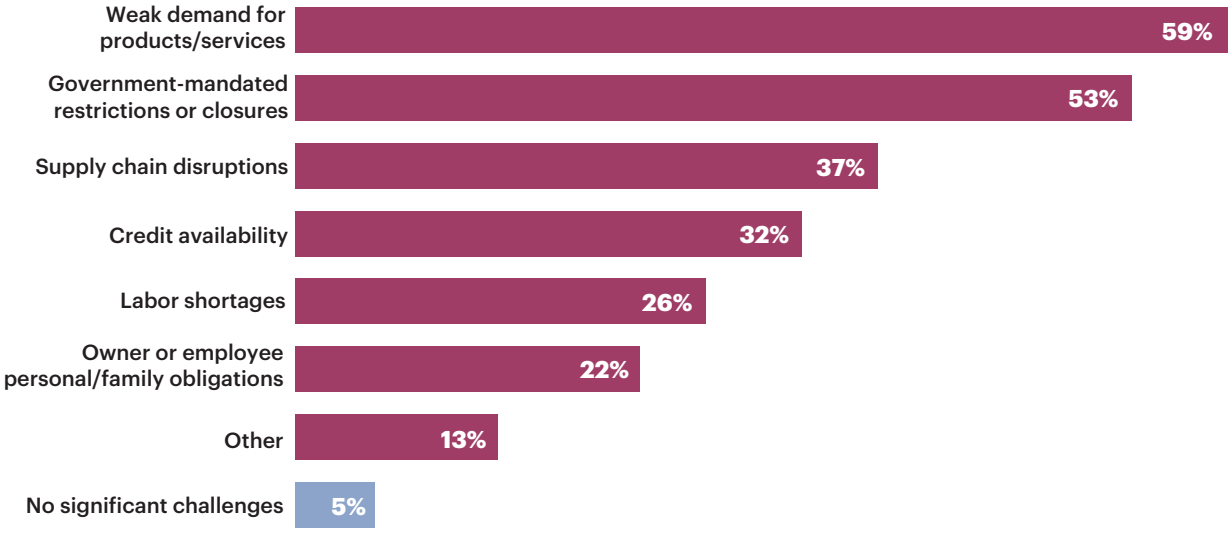
Fourth District community banks played a critical role in small business financing even prior to the pandemic. Small business loans made up over 4 percent of Fourth District community banks' assets as of December 31, 2019, twice that of U.S. commercial banks nationally (see Figure 8). Since the crisis, the small business loan share of Fourth District community bank assets has increased sharply, driven in part by PPP loans.

Finally, survey results reveal that the small businesses that were approved for at least some of the financing sought from community banks were generally satisfied with the service they received, with 81 percent of those small businesses reporting satisfaction, up from 79 percent in 2019. In contrast, the satisfaction rate for the small businesses that were approved for at least some of the financing sought from large banks was only 68 percent.

Future Small Business Credit Needs

The SBCS reveals that all businesses continue to face headwinds. According to the survey, 95 percent of the

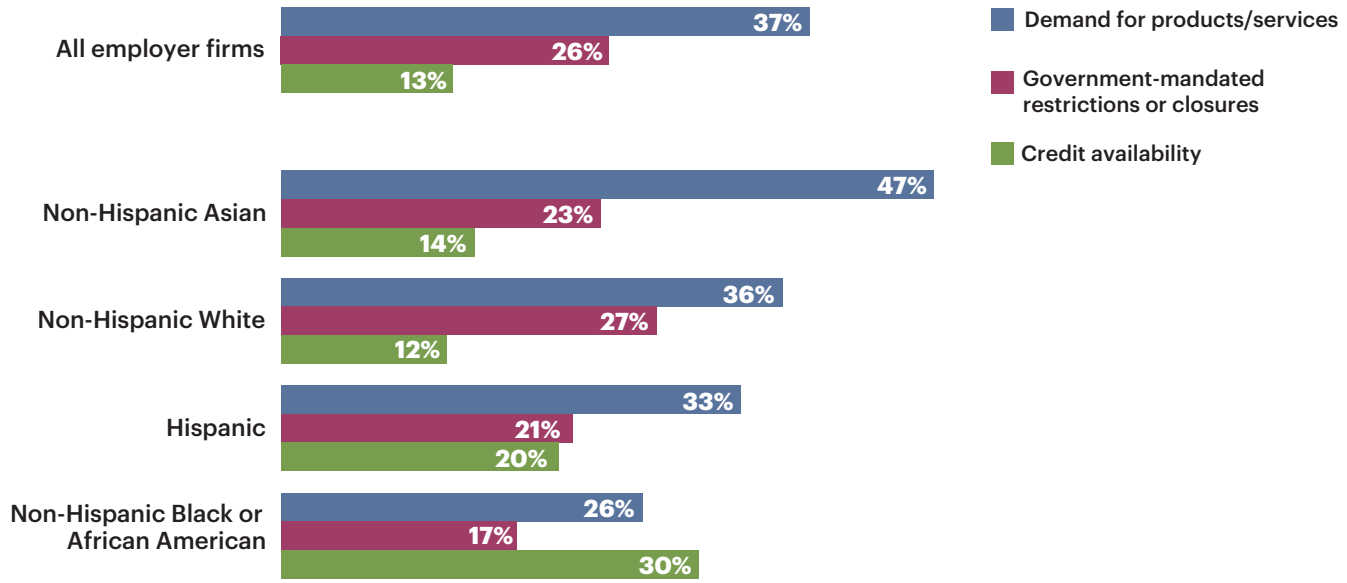
Figure 9: Challenges Firms Expect to Face as a Result of the Pandemic, Next 12 Months



Note: Respondents could select multiple options.

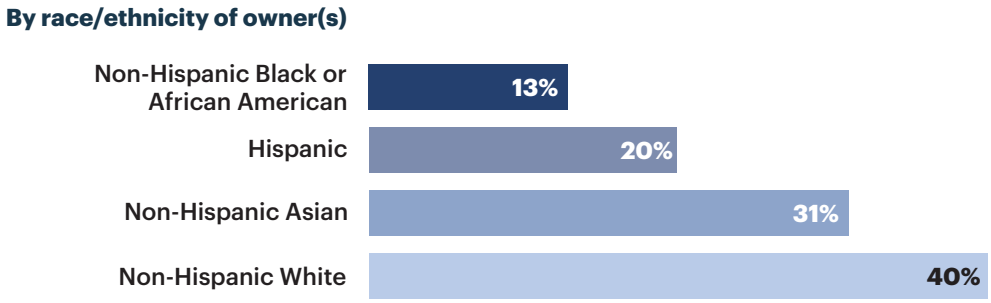
Source: *Small Business Credit Survey: 2021 Report on Employer Firms*

Figure 10: Single Most Important Challenge Firms Expect to Face as a Result of the Pandemic, Next 12 Months, Top Challenges Shown



Source: *Small Business Credit Survey: 2021 Report on Employer Firms*

Figure 11: Share of Firms That Received All Financing They Sought (% of applicants)



Source: *Small Business Credit Survey: 2021 Report on Employer Firms*

firms expected pandemic-related challenges to continue into the next 12 months; of those, 32 percent expect to face challenges with regard to credit availability (see Figure 9).

While weak demand remains the top concern for small businesses in the survey (see Figure 10), credit availability is the top concern for non-Hispanic Black– or African American–owned small businesses, and that concern is likely driven by the relatively low levels of funding received by these small business owners. As shown in Figure 11, only 13 percent of non-Hispanic Black– or African American–owned small businesses received all financing sought, compared with 40 percent of non-Hispanic White businesses.

Conclusions

Small businesses play a significant role in United States job creation. The Small Business Administration's (SBA) most recent Small Business Profiles show small businesses added 1.8 million net new jobs in the United States during 2019, the latest year studied.[11] According to the SBA profile, the United States has 30.7 million small businesses, and they employ 47.3 percent of the private workforce, and small businesses drive job creation.

As a result of the COVID-19 pandemic, small businesses experienced dramatic declines in both revenues and employment, and many business owners sacrificed personal assets to help their firms survive these unprecedented times. During the first six months of the pandemic, community banks played a central role in helping this important economic segment access government-provided emergency funding, as well as in providing private loans, lines of credit, and cash advances. Community banks received and approved more small business loan, line of credit, and cash advance applications than did their large bank counterparts.

Small business owners continue to face headwinds, however, and Black-owned small businesses report that credit availability remains a top concern. Serving this important segment and ensuring the ability of small businesses, particularly minority-owned small businesses, to equitably access credit will remain an important challenge for community banks and all financial institutions. ■

[11] The 2019 Small Business Profile is available at https://cdn.advocacy.sba.gov/wp-content/uploads/2019/04/23142719/2019-Small-Business-Profiles-US.pdf.

The Evolution of the Community Bank Business Model Series: Impact of Technology*

The Evolution of the Community Bank Business Model series kicks off with this article on the opportunities and unique challenges the evolving technology landscape presents to community bank innovation, competition, and achieving scale. This article also provides an update on regulators' actions to support community bank innovation.

The financial sector has historically embraced technological advances with varying degrees of enthusiasm and some pragmatism. Since the first automated teller machine was introduced more than 50 years ago, the industry has witnessed a shift to IT-based delivery systems, automated payment clearing, and internet banking as well as a proliferation of new financial products.[1,2] Emerging technologies (e.g., machine learning, natural language processing, cloud computing, robotic process automation, faster payments, and application program interfaces) continue to transform the banking industry and are increasingly important to how banks innovate and keep pace with competition in the industry from financial technology (fintech) firms, credit unions, and their peers.

Banks both large and small recognize the importance of technology investment. A 2018 Florida International University study showed that the median real technology spending per bank has doubled since 2000 for both small and large banks.[3] However, for similar proportional investment, this study noted that the payoff from technology investment differed, with large banks seeing a greater increase in operational efficiency, profit margins, and market value. The study noted that smaller banks still needed to adopt new technologies to remain competitive in the market.

Respondents (64 percent) of the Conference of State Bank Supervisors (CSBS) 2020 National Survey of Community Banks[4] viewed banks' adoption of new technologies as a necessity in delivering their products and services. However, a community bank's ability to adopt new technologies and innovate is dependent on its customers, its ability to acquire and develop staff expertise, and

* This article is the first of a two-part series based on research conducted in 2019 by Federal Reserve staff: Bettyann Griffith, Federal Reserve Bank of New York; Deeona Deoki, Federal Reserve Bank of New York; Chris Henderson, Federal Reserve Bank of Philadelphia; Chantel Gerardo, Federal Reserve Bank of Philadelphia; James Fuchs, Federal Reserve Bank of St. Louis; Mark Medeiros, Federal Reserve Bank of Atlanta; Justin Reuter, Federal Reserve Bank of Kansas City; Jonathan Rono, Board of Governors; and James Wilkinson, retired from the Federal Reserve Bank of Kansas City.

[1] See Elizabeth Judd, "Timeline: 180 Years of Banking Technology," *Independent Banker*, October 31, 2017, available at https://independentbanker.org/2017/10/timeline-180-years-of-banking-technology.

[2] See Allen N. Berger, "The Economic Effects of Technological Progress: Evidence from the Banking Industry," *Journal of Money, Credit and Banking,* 35(2) (April 2003), pp. 141–176, available at www.jstor.org/stable/3649852.

[3] Zifeng Feng and Zhongua Wu, "Technology Investment, Firm Performance and Market Value: Evidence from Banks," 2018, available at www.communitybanking.org/~/media/files/communitybanking/2018%20papers/session3_paper4_feng.pdf.

[4] Results of the survey were presented at the 2020 Community Banking in the 21st Century research and policy conference. See www.csbs.org/system/files/2020-09/cb21publication_2020.pdf.

partnerships with its core service provider (CSP), fintech firms, and other vendors.

The Competition

Community banks tend to demonstrate strength during times of crisis and uncertainty in part due to the strength of their relationships with customers, and they can leverage their experiences during these times to build for the long term in order to maintain or increase market share. Prior to the pandemic, community banks were losing ground to larger banks and nonbanks as customers sought faster access and a wider variety of lending and deposit options. For instance, over the past few years, community banks had been losing ground to bigger banks in small denomination business loans, a product commoditized by larger banks given that these loans do not require "soft" information about borrowers for approval.[5] Additionally, larger banks, which have deeper pockets and more technological strength, have taken advantage in gathering deposits through online channels that collect internet deposits.

Competition from nonbanks is increasingly another concern, as smaller banks are disproportionately affected by health savings accounts, peer-to-peer payments, automated investment platforms, and customer loyalty credit cards. Underscoring the competition from nonbanks is the re-emergence of industrial loan company charters and the creation of other related regulatory structures. In addition, credit unions have purchased an increasing number of community banks in the past decade. Additionally, due to a variety of factors, the number of community banks nationwide has declined by nearly 50 percent in the past two decades, going from 9,795 at the end of 2000 to 5,036 at the end 2019.[6]

[5] Data obtained from Reports of Condition and Income (Call Reports).

[6] Data obtained from S&P Global Market Intelligence.

At the beginning of the COVID-19 pandemic, there was a great deal of uncertainty as to how banks should adapt their operations in order to continue to serve their customers and communities. Despite the challenges of the pandemic, community banks shone a bright light on the importance of the relationship banking model as they successfully supported retail and small business customers. As community banks were compelled to temporarily close branches to keep customers and staff safe, technological interfaces that were already available but not used by large segments of customers were leveraged to great success. Further, community banks administered about 40 percent of the loans (by loan amount) in the 2020 Small Business Administration Paycheck Protection Program, which far exceeded their 15 percent representation in the banking industry by asset size.[7]

As the pandemic experience demonstrated, community banks can compete by designing their delivery of key banking products and services to meet ever-changing customer preferences, while maintaining essential elements of relationship-based lending.

The Customer

Community banks are challenged with serving a wide array of customers with varying needs. Many community banks are located in rural areas and serve an aging demographic, while younger potential customers migrate to larger cities for employment opportunities.[8] This challenge represents potential opportunities for community banks to build multiple channels, both physical and online, to deliver products to customers in their geographic markets and to expand into other markets.

[7] Data obtained from S&P Global Market Intelligence.

[8] Data from the 2010 Census highlight the unique demographic of rural communities. The results of the 2020 Census were not available at the time of the writing of this article to assess changes in the demographics from 2010.

Additionally, in the midst of the pandemic, through necessity, banks were able to reintroduce technology tools that were not heavily marketed in the past to customers who were hesitant to use them. Community banks could benefit from leveraging the momentum created by the pandemic to explore technologies to increase product and service offerings. This would not only benefit current customers but also serve to broaden the geographic and demographic reach of community banks and to gain new customers.

Talent Resource and Knowledge

While this may be an opportune time to encourage once-resistant customers to use more technologically advanced products and services, a bank's board of directors, senior management, and staff will also have to be adaptive to technological advances and associated risks. For instance, as banking services are made more available online, the risk of cyberattacks increases. Over the past few years, there has been a rise in reported cybersecurity incidents, such as the recent Finastra, SolarWinds, and Microsoft Exchange breaches. Given their geographic location, limited cybersecurity talent, and fierce competition for cybersecurity professionals driving up wages, community banks are challenged to hire or develop this necessary talent.

Another key risk continues to be managing third- and fourth-party vendor risks as banks leverage technologies to innovate and remain competitive. It will be important for a bank's board of directors and senior management to have a more nuanced understanding of technology services to ensure that they understand how their bank can continue to operate in a safe and sound manner. The bank's board of directors and senior management should understand who is responsible for which elements of the technology purchased from a provider (e.g., who owns the data, who is responsible for data protection, who has access to the data, and how the data can be used) to mitigate exposure to residual risks. In considering various technologies and business partners, a bank will need to understand its exit strategy, data privacy security requirements, contingency plans, and data retention policies. These risk factors also have implications for a bank's needs for talent and expertise among its board of directors, senior management, and staff.

Respondents to the 2020 CSBS survey expressed concern about the complexity of technological advances compared to the expertise of bank staff. Talent acquisition can be a challenge because community banks typically hire from their local communities and their geographic locations often make it difficult to access or attract talent with deep technological expertise. Additionally, community banks may not be able to compete with the compensation or training programs offered at larger banks.

While these challenges are daunting, the evolving conversation about the future of work and changing priorities toward work–life balance may present unique opportunities that community banks can leverage. In thinking about these issues, community banks should consider evolving their human capital strategies to address the challenge of hiring staff with the requisite technical skills.

Core Service Providers (CSPs)

Perhaps the biggest challenge to innovation is a community bank's access to technology services that are aligned with its strategic plan and budget. Given their size and resources, most community banks source their technology platforms from CSPs. Therefore, community banks tend to be reliant on CSPs' abilities to innovate and provide scale, though there is a limited number of CSPs from which to choose.

CSPs tend to invest in product development either through mergers and acquisitions of fintech firms or through research and development; however, it is difficult to measure the pace of their innovation in comparison to the broader financial services industry. Although community banks are generally satisfied with the basic services (e.g., risk management, security) of their CSPs, according to the CSBS survey, they are interested in innovation through expanded product offerings to achieve efficiency and scale. This increases the opportunities for new partnerships between fintech firms and community banks because fintechs are providing new ways for community banks to innovate and compete (from automated mortgage and auto loan origination to anti-money laundering transaction monitoring). A community bank's ability to partner with these firms and take advantage of these new technologies, however, is sometimes dependent on its CSP's openness to third-party providers and scalability of the core platform.

Therefore, it is important for community bank leadership to have a good understanding of its CSP's technical capability and the details of contractual obligations, especially when considering terminating the relationship with a CSP or entering into a partnership with a fintech firm. Service contracts with CSPs can include legal and financial barriers for early termination, and there are high operational costs to migrating to new platforms. According to the 2020 CSBS survey, 47 percent of the respondents were dissatisfied or highly dissatisfied with the flexibility offered by their CSPs, 40 percent of the respondents were dissatisfied or highly dissatisfied with the cost of their core processing services, and 40 percent were dissatisfied or highly dissatisfied with the speed of innovation at their CSP. In addition, the use of an open application program interface (API) to facilitate fintech firms' connection with CSP systems is key for community banks when engaging with fintech firms. While APIs are not new and come with challenges, including security threats, system compatibility, and expertise requirements, their increasing usage and importance makes them transformational and an important factor in the discussion between a community bank and its CSP.

With the proliferation of technology, community banks may need to assess the products and services offered by their CSPs. Therefore, banks will need to actively manage the relationship to ensure their CSPs deliver a robust suite of technologically advanced products and services, either directly or indirectly, through connections to third-party vendors and fintech firms. With more to gain, community banks could use their collective voice to demand more from their technology partners, particularly CSPs.

There is a cost element associated with innovation; community banks and CSPs will have to weigh the costs and benefits of innovation to reach acceptable solutions for both parties.

A Comprehensive Business Strategy

A comprehensive business strategy that articulates a clear case for new or existing products and services based on client needs and growth opportunities is important for community banks. Such a strategy would help them compete in a changing and competitive landscape and address the challenges discussed in this article.

The business strategy can:

- position a bank to achieve the agility required to support existing and new customers both inside and outside of the bank's immediate geographic location.
- organize a bank to use the momentum coming out of the pandemic to help customers get comfortable with using more advanced technologies.
- provide a risk management framework (that includes managing technology and cyber risks, third- and fourth-party vendor risks, and risks related to product specializations) to ensure that bank staff and

management teams are prepared to operate in this new and rapidly changing environment.

- prepare a bank for attracting and retaining clients as well as acquiring and retaining talent. This includes expanding its human capital strategy to ensure that bank staff have necessary technical skills and expertise through training or hiring.
- help a bank actively manage its relationships with third-party service providers, including its CSP. Community banks should ensure that CSPs are not limiting their technological innovation.

Regulators' Actions

Regulators are committed to engaging with community banks and providing resources to support the innovation of community banks as they navigate the challenges of the evolving banking environment. The following are a few Federal Reserve System and interagency initiatives:

Innovation Office Hours — In 2020, the Federal Reserve began hosting these sessions to facilitate face-to-face discussions on innovation in the financial services with supervised financial institutions, fintech firms, Federal Reserve staff, and other industry participants. Innovation Office Hours can be two-way learning opportunities for both the firms and Federal Reserve staff. Sessions were held in June and September of 2021, with more to be scheduled in 2022. Community banks are encouraged to attend the sessions hosted in their District. For more information, refer to the Innovation page on the Federal Reserve Board's website.[9]

Fintech Partnership Staff Paper — As Governor Michelle W. Bowman referenced in the first issue of 2021 of *Community Banking Connections*, Federal Reserve Board staff held discussions with community banks, technology companies, and other relevant stakeholders to gather their perspectives on the evolving landscape of community bank partnerships with fintech firms. Board staff distilled key insights in a public paper to serve as a resource to community banks considering fintech partnerships. To access this resource, refer to the Board of Governors' website.[10]

Community Bank and Service Provider Series — In September 2021, the Federal Reserve System hosted the first session in the series to help community banks build a stronger understanding of the value and risks associated with fintech firms and their intersection with CSPs. This session was a mechanism to help community banks build their collective voice when engaging with service providers. Refer to the Ask the Fed website.[11]

Conducting Due Diligence on Fintech Firms: A Guide for Community Banks — The Federal Reserve, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation recently issued an interagency due diligence optional guide to serve as a resource to community banks as they conduct due diligence on potential fintech partners. The guide is intended to serve as a starting point in the due diligence process and is not intended to create new regulatory expectations. To access this resource, refer to the Board of Governors' Supervision and Regulation Letters page.[12]

Conclusion

As the U.S. banking industry has evolved, community banks have largely managed to retain their distinctive attributes and remain an enduring feature of the broader financial system. Still, they are not immune to the intense competitive forces of the 21st century. It is up to community banks to understand these challenges and opportunities to ensure they are appropriately responsive and adaptive.

The second article in this series will discuss the challenges of rural banks in comparison to their urban counterparts with a focus on operational differences between the cohorts. ■

[9] The Innovation page is available at www.federalreserve.gov/aboutthefed/innovation-office-hours-series.htm.

[10] See www.federalreserve.gov/newsevents/pressreleases/bcreg20210909a.htm.

[11] The website is available at https://bsr.stlouisfed.org/askthefed.

[12] See www.federalreserve.gov/supervisionreg/srletters/srletters.htm.

Endpoint Security: On the Frontline of Cyber Risk

by Ahmed Hussain, Risk Management Specialist, Supervision and Regulation, Federal Reserve Bank of Chicago, William Mark, Lead Examiner, Supervision and Regulation, Federal Reserve Bank of Chicago, and Anthony Toins, Senior Examiner, Supervision and Regulation, Federal Reserve Bank of Chicago

Endpoint devices, such as desktops, laptops, servers, routers, and mobile devices, can be susceptible to malicious cyberattacks and breaches. Endpoint devices remain primary targets for attackers and, therefore, are vulnerable points of entry to any community bank's network. Given this, a major priority for any endpoint security effort is the protection of endpoint devices. These devices present a daunting challenge because they are typically under the control of and in use by employees, providing remote communication with and connection to a bank's network. Endpoint security and related employee training represent the frontline of a multilayered, defense-in-depth strategy against cyberattacks.

The COVID-19 pandemic has exponentially increased the number of employees engaging in or transitioning to remote work, a trend likely to continue for years to come. A study conducted by the Enterprise Strategy Group (ESG) reported that 76 percent of information technology (IT) professionals on average across all respondent companies are currently working from home. Moreover, 57 percent of the IT professionals surveyed were amenable to increasing their level of remote work in the post-pandemic environment.[1]

The portability of endpoint devices, coupled with the surge of remote work, increases a bank's risk exposure to cyber breaches due to potential susceptibility to theft or misplacement. One-third of remote workers believe that they have not received sufficient cyber awareness training to work safely and efficiently from home, according to the ESG study. Unclear staff guidance and understanding can further exacerbate this weakness by fostering uncertainty, thereby leading to cybersecurity mistakes.

In this fashion, IT hygiene, which "provides visibility into the 'who, what and where' of your environment while giving you the means to address security risks before they become issues,"[2] may be lacking. In other words, a bank may not be fully able to recognize "who" is breaching the network, "what" methods are being used, and "where" these vulnerable endpoints are.

As discussed in a joint statement issued by the United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC), a growing number of cybercriminals and other malicious groups are actively exploiting the current virtual environment by targeting endpoint vulnerabilities.[3] A wide range of cyberthreats, such as malware, phishing, and other premeditated attacks, challenges organizations to remain technologically current and maintain diligent staff cyber awareness to ward off such incursions.

Since the beginning of the COVID-19 pandemic, an exponential increase across the spectrum of cyberattacks has challenged organizations. Some observers coined the term *cyber pandemic* to characterize the current evolving cyber environment.[4] The Federal Bureau of Investigation (FBI) reported in its 2020 Internet Crime Report that, compared with 2019, complaints of suspected internet crime ballooned by over 300,000, to nearly 800,000 incidents, leading to aggregate reported losses in excess

[1] See Bill Lundell, "ESG Research Report: The Impact of the COVID-19 Pandemic on Remote Work, 2020 IT Spending, and Future Tech Strategies," June 16, 2020, available at www.esg-global.com/research/esg-research-report-the-impact-of-the-covid-19-pandemic-on-remote-work-2020-it-spending-and-future-tech-strategies.

[2] See "Why IT Hygiene Is Critical to Your Cybersecurity Readiness," *CrowdStrike* blog, June 14, 2017, available at www.crowdstrike.com/blog/why-it-hygiene-is-critical-to-your-cybersecurity-readiness.

[3] See the April 8, 2020, joint statement by the NCSC and CISA, "UK and US Security Agencies Issue COVID-19 Cyber Threat Update," available at www.cisa.gov/news/2020/04/08/uk-and-us-security-agencies-issue-covid-19-cyber-threat-update.

[4] See Daniel Lohrmann, "2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic," *Government Technology* blog, December 11, 2020, available at www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html.

of $4.2 billion.[5] Such malicious activity is not expected to abate in 2021, as cyberattack attempts are projected to increase to every 11 seconds, more than double the frequency of every 39 seconds noted in 2019.[6] Observers project damages from cyber events could reach $6 trillion in 2021 globally.[7]

Federal Reserve Vice Chair for Supervision Randal K. Quarles said at the Financial Services Roundtable 2018 Spring Conference in Washington, D.C., "While we know that successful cyberattacks are often connected to poor basic IT hygiene, and firms must continue to devote resources to these basics, we also know that attackers always work to be a step ahead, and we need to prepare for cyber events."[8] Although Vice Chair for Supervision Quarles delivered these comments in a fundamentally different environment, they remain relevant today. Diligent endpoint security efforts are needed now more than ever to help identify and mitigate risks posed by cyberthreats.

What Is Endpoint Security?

Endpoint security practices are a vital component for safeguarding endpoint devices and enterprise networks. The ultimate goal is to protect the confidentiality, integrity, and availability of network information by closing the loopholes that attackers may exploit to gain unauthorized access.

The Ponemon Institute estimated that these data breaches have an average cost of nearly $4 million per incident.[9] Additionally, data breaches can have detrimental impacts beyond financial costs. They can also lead to the loss of personally identifiable customer information, reputational damage to a firm, and potential legal issues. Consider the 2017 Equifax data breach, one of the largest breaches in history, affecting nearly 150 million consumers. This breach occurred as a result of a preventable lapse in basic protocols, a missed systems patch.[10]

According to Absolute Software Corporation, 70 percent of all breaches originate through endpoints,[11] so related endpoint security measures are critical in managing cyber risks. With the increase in such incidents at endpoints, multilayered defenses are important to ensure that a bank's network has a robust security environment. Because sophisticated cyberthreats are on the rise, IT managers and administrators need to more carefully assess the extent to which security gaps in deployed endpoint devices may expose the network to excessive risks.

Endpoint Risks

As mentioned, endpoints are usually the preferred targets for cybercriminals. Remote devices are especially vulnerable due to the sheer volume of users, which fosters greater opportunities to exploit an endpoint, making them attractive targets to hackers. Endpoint devices provide points of entry to access corporate networks, so they are susceptible to cyberattacks designed to steal or encrypt data or even take control of a device to execute an attack.

Today, endpoint devices and their users pose a myriad of threat scenarios, such as zero-day vulnerabilities,[12] malware, ransomware, and phishing. Hackers exploit these weaknesses to circumvent existing detection systems and take advantage of flaws in popular software. Most cyberattacks are engineered through phishing and pose the highest risk to endpoint devices. This could involve an

[5] See the FBI Internet Crime Complaint Center's "2020 Internet Crime Report," available at www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

[6] See Allan Jay, "73 Important Cybercrime Statistics: 2020/2021 Data Analysis & Projections," FinancesOnline, available at https://financesonline.com/cybercrime-statistics.

[7] See "30 Practical Cybersecurity Statistics to Be Wary of in 2021," *Safe at Last* blog, available at https://safeatlast.co/blog/cybersecurity-statistics.

[8] Read the text of Vice Chair for Supervision Quarles's February 26, 2018, speech, "Brief Thoughts on the Financial Regulatory System and Cybersecurity," at www.federalreserve.gov/newsevents/speech/quarles20180226b.htm.

[9] See IBM, "2020 Cost of a Data Breach Report," available at www.ibm.com/security/data-breach.

[10] See Zack Whittaker, "Equifax Breach Was 'Entirely Preventable' Had It Used Basic Security Measures, Says House Report," TechCrunch, December 10, 2018, available at https://techcrunch.com/2018/12/10/equifax-breach-preventable-house-oversight-report.

[11] See Louis Columbus, "5 Key Insights from Absolute's 2019 Endpoint Security Trends Report," *Software Strategies Blog*, September 20, 2019, available at https://softwarestrategiesblog.com/2019/09/20/5-key-insights-from-absolutes-2019-endpoint-security-trends-report/.

[12] *Zero-day vulnerability* is a software security flaw that is known to the software vendor but that no patch is in place to fix. If this software flaw is left unaddressed, security holes are created that cybercriminals can exploit.

employee downloading a suspect application or clicking on an email link or attachment that connects to malware or ransomware. Credential theft, social attacks (i.e., phishing and business email compromise), and associated events account for 67 percent of all cyber breaches.[13] Consequently, traditional centralized security measures alone are no longer sufficient for protecting a mobile workforce.

Certain endpoint devices can pose more risk than others due to the nature of their use. For example, remote endpoints generally are inherently riskier and subject to cyberattacks because they are often used by employees who are traveling or working remotely and more likely to connect to less-secure public Wi-Fi. Endpoint devices such as laptops, tablets, and smartphones are, by virtue of their portable nature, at higher risk of being lost or stolen. As noted in the Figure, laptops were among the most compromised endpoints in 2019. While endpoint devices generally present a notable risk to an organization's network, such devices enable financial institutions to serve their customers in a timely and efficient manner.

Endpoint security is even more relevant as more organizations adopt "bring your own device" (BYOD) processes, which allow employees to connect personal mobile devices to an organization's network. These personal devices tend to have additional risks associated with lack of information security control, such as downloaded malicious applications, improper password control, and storage of sensitive data, if not appropriately configured or controlled. Institutions should determine whether existing BYOD security controls are sufficient and, at a minimum, ensure that practices such as application controls, feature controls, encryption, remote wipe capability, storage control, malware protection, and proper password control are in place to protect devices from these added risks.

Attack Vectors

Cybercriminals use attack vectors as routes to infiltrate an organization's network. To protect against these unauthorized incursions, IT administrators rely on risk assessments to monitor and document any changes to the internal network (i.e., architecture, configurations, remote workers) and external factors (i.e., heightened cyber risk environment) in order to recognize potential attack vectors in a timely fashion. Most attack vectors share commonalities, as attackers typically:

1. identify a potential target;
2. gather information about the target (e.g., using social engineering, phishing, malware, automatic vulnerability scanning);
3. analyze gathered information to identify potential attack vectors with tailored exploitation tools;
4. gain unauthorized system access to steal data or install malicious code; and
5. monitor a computer or network in order to acquire information or use computing resources.

Prior to the onset of the pandemic and the widespread work from home posture, financial institutions regularly conducted business via mobile devices, which widened the network perimeter and attack surface.

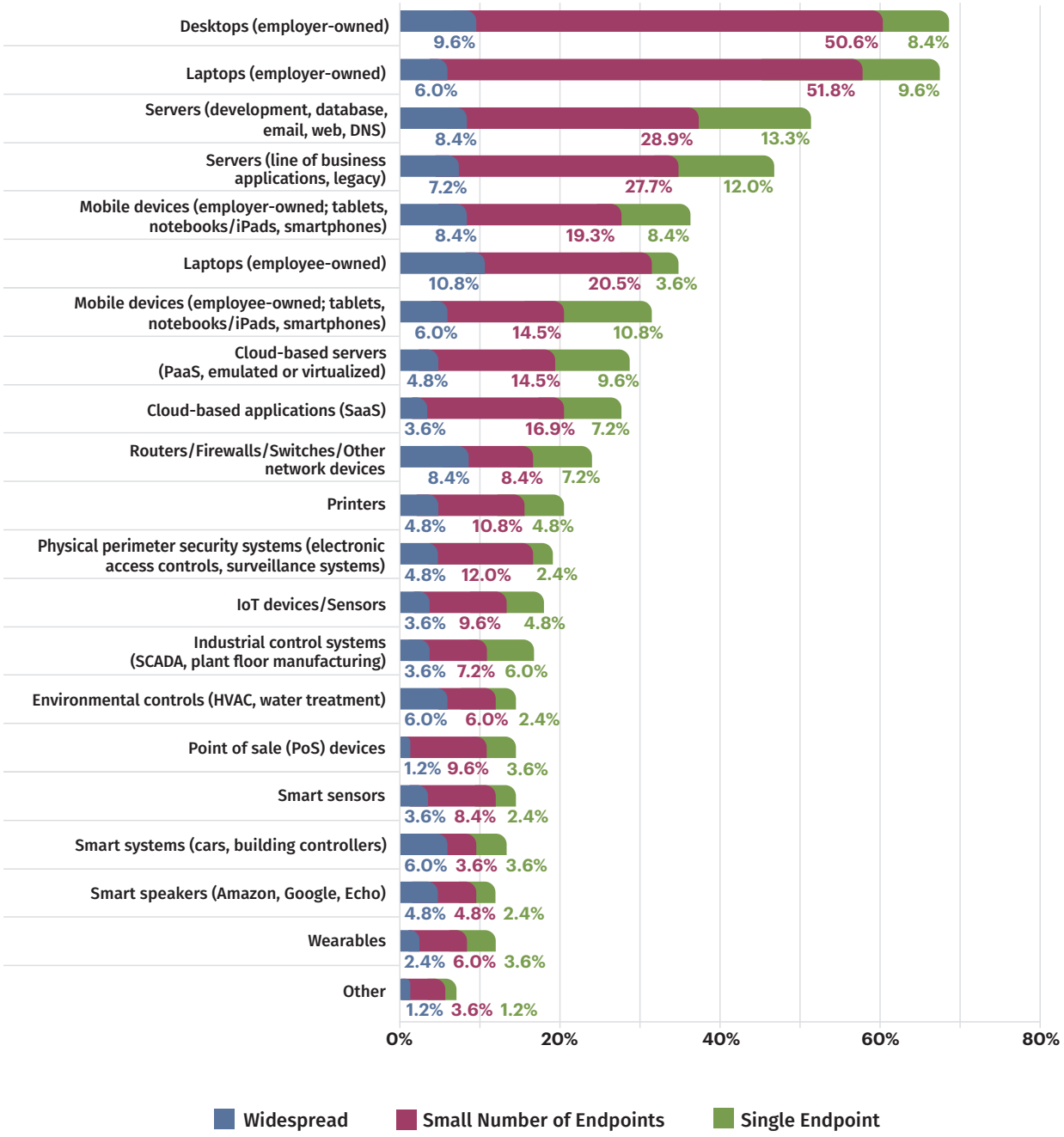
In the current heightened cyber risk environment, securing endpoints is paramount and any delays could mean the loss of data confidentiality, integrity, and availability. Although endpoint devices are often connected to the enterprise network through a secure channel, such as a virtual private network (VPN), these devices remain attractive targets. As a result, bank management should consider the increased cybersecurity risks posed to the bank and its customers. The FBI reports that scammers are leveraging the COVID-19 pandemic to steal funds, personal information, or both.[14] Therefore, a bank should be intentional in reminding its employees to scrutinize all emails from outside sources. While electronic messages that purport to provide information on COVID-19 may be enticing, the downside risks of clicking on a link for a false online charity, opening an attachment from known or unknown sources, or sending personal or confidential information to receive money or other benefits can be significant.

[13] The Verizon 2020 Data Breach Investigations Report is available at https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf.

[14] See Calvin A. Shivers, "COVID-19 Fraud: Law Enforcement's Response to Those Exploiting the Pandemic," Statement Before the Senate Judiciary Committee, Washington, D.C., June 9, 2020, available at www.fbi.gov/news/testimony/covid-19-fraud-law-enforcements-response-to-those-exploiting-the-pandemic.

Figure: 2019 SANS Survey — Types of Endpoints Compromised

Over the past 12 months, what types of endpoints have been compromised? Respondents were asked to indicate if these were widespread or limited in scope to either a small number of endpoints or just one endpoint.



Note: *Domain name system* (DNS) is the system for tracking and regulating internet domain names and addresses; *internet of things* (IoT) is the interconnection among computing devices in everyday objects that facilitate data transfer through the internet; *platform as a service* (PaaS) refers to a cloud computing service platform that allows customers to develop, run, and manage applications without building and maintaining their own application infrastructure; *software as a service* (SaaS) is a software licensing and delivery model in which software is licensed on a subscription basis and centrally hosted; and *supervisory control and data acquisition* (SCADA) is a powerful computer system that allows users to monitor and control processes in real time remotely.

Source: SANS Institute, *2019 SANS Survey on Next-Generation Endpoint Risk and Protections*

Implementing Endpoint Security

With new types of attacks and complex threats emerging each year, methodologies to protect endpoint devices continue to evolve. Today, vigilant endpoint security includes sophisticated detection and analytical tools to identify gaps that attacks could exploit and where bank defenses may lag. Many approaches and techniques may be used to initiate endpoint security using a multilayered threat protection strategy.

Effective endpoint security starts with understanding an institution's operating environment and what applications and devices will be allowed on the network. IT administrators should identify and validate all network entry and exit points and address such exposures prior to implementation. Endpoint security threats may be countered through a network policy-based approach, especially the prevention of installation and use of high-risk applications such as file sharing, social media applications, and connections to unauthorized devices. This approach ensures that endpoint devices meet specific criteria or rules governing all endpoints before network access is granted.[15] For example, all remote endpoint devices could be required to undergo a vulnerability scan prior to being allowed to connect to a bank's network resources. In turn, this policy-based approach would allow the bank to quarantine any noncompliant endpoints before there is a network connection.

Applications of endpoint security solutions and tools are necessary components in combatting network threats. These processes work by understanding how endpoint security tools interact with potential threats and network resources. Many options are available, and several strategies may be applied when considering security solutions to deploy. IT administrators typically use an array of applications that detect advanced threats, such as malware, zero-day incursions, and fileless attacks, to protect a bank's network.

Strategic failures often arise from inadequate understanding by IT administrators of all the possible ways an intruder could penetrate the network and the various capabilities of existing applications. IT administrators should choose comprehensive security offerings that clearly define physical and virtual devices as well as provide desired defense against modern multivector threats.[16] Although no single solution offers protection from all endpoint risks, employing advanced security solutions and enterprise suites that use multiple methodologies is a prudent measure to "right-size" the degree of safeguards with cost considerations.

Institutions have a variety of standardized tools to consider when looking to properly align cybersecurity preparedness with common industry standards and practices. In a 2019 press release,[17] the Federal Financial Institutions Examination Council (FFIEC) referenced several useful standardization tools that offer methods to measure inherent risks and compare them with current controls to better assess the maturity and prospective capability of cybersecurity preparedness:

- Center for Internet Security (CIS) Controls[18]
- FFIEC Cybersecurity Assessment Tool (CAT)[19]
- Financial Services Sector Coordinating Council (FSSCC) Cybersecurity Profile[20]
- National Institute of Standards and Technology (NIST) Cybersecurity Framework[21]

From a community bank perspective, addressing these challenges may seem daunting and management may find that it has insufficient staff expertise. Targeted training initiatives could bridge the knowledge gap and facilitate staff vigilance. Outsourcing IT administration is an option employed by banks; however, this choice does not absolve the board of directors and management of responsibility for oversight of cybersecurity efforts. Diligence in vendor risk management is also important to ensure that a bank

15 See TechTarget definition, "Endpoint Security Management," https://searchsecurity.techtarget.com/definition/endpoint-security-management.

16 See Webroot, Inc., "Understanding Endpoints and Endpoint Security," available at www.webroot.com/us/en/resources/glossary/what-is-endpoint-security.

17 The FFIEC's August 28, 2019, press release, "FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness," is available at www.ffiec.gov/press/pr082819.htm.

18 See "CIS Controls," available at www.cisecurity.org/controls.

19 The FFIEC May 2017 CAT is available at www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf.

20 The FSSCC Cybersecurity Profile can be found at https://cyberriskinstitute.org/the-profile.

21 The NIST Cybersecurity Framework is available at www.nist.gov/cyberframework.

has appropriate oversight and adequate controls in place to confirm that any third party provides the necessary services to achieve cybersecurity goals.[22]

Observed Industry Practices

There is no single solution that can prevent every attack; however, solutions properly configured and promptly implemented within an effective cyber awareness program can deter or effectively slow an attack to allow a bank to detect the attack in order to take defensive action. With a greater potential for an attack due to the surge of remote work, community banks should employ industry-recognized endpoint security measures to keep sensitive data safe. The following are several common industry practices to consider:

1. **Identify all network endpoints**
   To ensure visibility into all endpoints in the network, it is important to identify and inventory all endpoints. Each one represents a door or potential vulnerability that can be exploited to gain network access.

2. **Enforce principle of least privilege[23]**
   Least privilege is the practice of limiting user access to networks, systems, and programs to only employees needing access to complete given tasks. Under this principle, each employee is given only the minimum privileges or permissions associated with an assigned role and administrative access is limited to employees whose duties require it. This is particularly effective in limiting the spread of malware infections.

3. **Disable unnecessary ports**
   Unsecured or open network ports often go unmonitored and are vulnerable to unauthorized intrusion. Additionally, neglected communication ports, such as Bluetooth, infrared devices, and modems, have been the entry point for many recent destructive cyberattacks; these ports should be identified and the configurations or settings adjusted to disable potential access. Periodic scans should be performed, especially when new hardware and applications are incorporated into the IT environment, to determine which network ports are open, what services are running, and whether internet access is sufficiently controlled.

4. **Employ mobile device management (MDM)[24]**
   The prevalence of mobile devices (e.g., laptops, phones, tablets) comes with increased attack surfaces and threat vectors. Vigilant MDM can secure access to these devices and, when necessary, wipe a device remotely, keep software updated, encrypt data, log and track usage, prevent file sharing and downloading of unauthorized applications, and ensure that suspicious applications are opened in a secure and safe manner (i.e., sandboxing[25]).

5. **Exercise application control[26]**
   Application control is a security technology that can allow or restrict communication between applications and network devices within an organizational network. In addition, to ensure that only trusted communications are passing through endpoints into an organization's network, IT administrators can create a list of trusted programs, scripts, and processes or a list of those banned. Such lists are particularly useful for securing networks from BYODs.

6. **Strengthen identity and access management**
   Practices to ensure proper identity and access management are best applied with a layered defensive approach that includes: (a) "zero-trust"[27] strategies; (b) multifactor authentication; (c) strong password policy enforcement; (d) timely removal of unnecessary applications, devices, and users; and (e) periodic audits.

[22] See Supervision and Regulation letter 13-19/Consumer Affairs letter 13-21, "Guidance on Managing Outsourcing Risk," available at www.federalreserve.gov/supervisionreg/srletters/sr1319.htm.

[23] See CIS, "Election Security Spotlight – Principle of Least Privilege," available at www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-principle-of-least-privilege.

[24] See CIS Controls Mobile Companion Guide, version 7, available at www.cisecurity.org/white-papers/cis-controls-mobile-companion-guide-2/.

[25] *Sandboxing* is a computer security term referring to setting aside a program in an environment isolated from other programs so that security issues that arise will not spread to other areas on the computer or network.

[26] See Check Point Software Technologies Ltd. Cyber Hub, "What Is Application Control?," available at www.checkpoint.com/cyber-hub/network-security/what-is-application-control/.

[27] *Zero-trust* is a security concept that restricts access to the network, applications, hardware, and devices to only known sources.

7. **Implement advanced protection against attacks**[28]
   To address increased complexity associated with ever-expanding infrastructures and an increased volume of deployed endpoints, timely automated responses to cyberattacks are important to minimize the adverse effect of intrusions. Endpoint protection platform remedies, which prevent malware attacks at the point of entry, and endpoint detection and response solutions, to discover and respond to threats that elude antivirus defenses, are designed to work in tandem to optimize protection.

8. **Patch systems promptly**
   Timely installation of software updates or patches can shore up network weaknesses so that they do not deteriorate into exploited endpoints.

9. **Provide security awareness training**
   Security awareness is paramount given that humans are the primary targets and vectors for entry into the network, typically through phishing and other social engineering attacks. A formal educational initiative propagating cyber knowledge with periodic reminders would be appropriate to establish and reinforce cyber vigilance.

10. **Promote location awareness**[29]
    A necessity associated with increased remote work is the capability of portable devices to allow both the user and the network administrator ability to actively or passively monitor and communicate location information in real time, thus enabling adaptability to security challenges in specific settings.

11. **Plan for incident response**
    Despite diligent endpoint security efforts, breaches may occur, so management should be organized and deliberate to ensure that, when a breach is identified, corrective measures are undertaken to prevent further loss in a timely, efficient, and thorough manner.

Conclusion

Today, employees are working from home at unprecedented levels due to the pandemic and relying on a diverse range of hardware and software tools to execute everyday tasks. As the volume and sophistication of cybersecurity threats have steadily grown, so has the need for robust endpoint security. The portability of endpoint devices and the sheer volume of usage have heightened risk to institutional networks. Limited cyber awareness can exacerbate these vulnerabilities.

It is incumbent upon bank management to implement endpoint protection systems designed to quickly detect, analyze, block, and contain attacks in progress. To accomplish this, collaboration with technology or managed security service providers, as well as consideration of other security technologies and platforms, would give IT administrators knowledge about global threats, improving detection and remediation response times. Adopting endpoint security tools is a good place to start, but it should be part of a wider strategy of ensuring cybersecurity hygiene that includes a diligent awareness program. An evolving, well-informed, and vigilant endpoint security program will require more than a single approach and, more important, demonstrate adaptability. Together with a disciplined incident response plan to address breaches in a timely fashion, such a program can go a long way to promote data confidentiality, integrity, and availability.

Federal Reserve Governor Michelle W. Bowman summarized the current environment at the 2020 Independent Community Bankers of America ThinkTECH Policy Summit: "There are certain points in history when an event can fundamentally change how society and entire industries function. In addition to the other ways that COVID-19 has affected us, this could be one of those moments. The pandemic has demonstrated the importance and unique role of technology in responding effectively to new challenges."[30] ■

[28] See Cisco Systems, Inc., "What Is an Endpoint Protection Platform (EPP)?," available at www.cisco.com/c/en/us/products/security/what-is-endpoint-protection-platform.html.

[29] See ScienceDirect.com definition, "Location Awareness," available at www.sciencedirect.com/topics/computer-science/location-awareness.

[30] Read the text of Governor Bowman's December 4, 2020, speech, "Technology and the Regulatory Agenda for Community Banking," at www.federalreserve.gov/newsevents/speech/bowman20201204a.htm.

2021 Writers' Cohort

Meet a Cohort Member

The past several issues of *Community Banking Connections* have featured profiles of members of the publication's Writers' Cohort, which was formed in 2019. In this issue, Alex Shelton discusses how taking an economics class taught by Marvin Goodfriend influenced his decision to join the Fed and why the trail system around the James River is one of the best "perks" of working for the Richmond Fed.

Alex Shelton

Portfolio Central Point of Contact/Senior Examiner, Supervision, Regulation, and Credit, FRB Richmond

How did you start your career with the Fed?

My career at the Fed began in 2010 when I became a senior condition monitoring analyst in the Credit Risk Management Department. Back then, I used my prior regulatory experience at the Federal Housing Finance Agency to help administer the Fed's payment system and the discount window. But my path to the Fed began much further back during my undergraduate days at the University of Virginia. One of the main concentrations for economics majors at UVA was public policy economics — predicting and understanding how individuals and organizations respond to various government programs. As part of this coursework, I took a graduate-level class in empirical monetary economics taught by Marvin Goodfriend, who, at the time, was vice president for research at the Federal Reserve Bank of Richmond. His passion for economics made him an outstanding teacher, ultimately influencing me to join the Fed.

What activity are you most passionate about?

Running! To me, running is a perfect combination of exercise and friendship. If you set up a good training program and stick to it with the help of friends, you can accomplish all the goals you have. I have completed six marathons to date, including the New York City

and Marine Corps marathons, and countless other races. I have organized weekly running groups from the Richmond Fed's building and captained a team of 12 to run across the Commonwealth of Virginia seven times (about 1,500 miles in total). In fact, the trail system surrounding the James River in Richmond is one of the best "perks" of working for the Fed. I've even arrived at work around 5 a.m. to complete an 18-mile training run before making my first meeting.

How long have you been running and how did you get interested in running?

I didn't get the running bug until 2012 when I ran in the Monument 10K, a race with more than 30,000 participants here in Richmond. A local YMCA sponsored a training team for the event, and most of their runs went through my neighborhood. I was fascinated by the variety of people I saw, from the speedy folks to the slower tortoises (a group I identified with). So I decided to give running a go. Before signing up for that race, I hadn't run since high school — and that was only when my coaches were upset with me. But what I liked the most about that group was the amazing comradery among all the runners. Maybe it's the shared misery and suffering, but the cumulative craziness is palpable. From there, my drive to continue running has been the search for the next personal best distance or a faster event time.

If you could take a month off and go running without worrying about expenses, where (in the world) would you choose to go? Also, why would you go there?

I have been infatuated with the running trails in the Pacific Northwest. I follow many ultramarathoners (folks that run more than 26.2 miles in a race), and the places they run are simply otherworldly to me. Whether it's the Coast Mountains of British Columbia or the Central Cascades of Washington State, the trail systems would take me through dense forests, across glacial rivers, and up to elevations that would dwarf anything I've been on before. Plus, the sheer concept of pushing past the marathon distance is daunting and exhilarating at the same time. Although I would need to "not worry" about the elevation as well as the expense. I was fortunate to complete a trail half marathon in Moab, UT, just before the pandemic, and even at just 4,000 feet above sea level — I was crushed! Little to say, the mountains around Vancouver are a little higher than that. ■

Cohort Chairs:

Ben Clem, Senior Manager, Supervision, Regulation, and Credit, FRB Richmond
Jennifer Grier, Senior Examiner, Supervision, Regulation, and Credit, FRB Atlanta

Cohort Members:

Kerri Allen, Examiner, Examinations & Inspections, FRB Kansas City, **Anthony Gonitzke**, Senior Examiner, Financial Institution Supervision and Credit, FRB San Francisco, **Jordan Jhamb**, Financial Analysis Associate, RCFI, FRB New York, **William Mark**, Lead Examiner, Supervision and Regulation, FRB Chicago, **Kalyn Neal**, Examiner/Supervisory Specialist, Examinations & Inspections, FRB Kansas City, **Alex Shelton**, Portfolio Central Point of Contact/Senior Examiner, Supervision, Regulation, and Credit, FRB Richmond, **Scott Zurborg**, Senior Large Bank Examiner, Supervision and Regulation, FRB Chicago

Federal Reserve's SCALE Method

On July 15, 2021, the Federal Reserve introduced a method and tool to aid community banks in implementing the current expected credit losses (CECL) accounting standard. This initiative is part of the broader work undertaken by the Federal Reserve System's Small Bank Supervision Working Group (SBSWG), a team of community bank supervision experts. In 2019, Federal Reserve Governor Michelle W. Bowman formed the SBSWG to identify initiatives that have the potential to reduce regulatory burden, improve supervisory effectiveness, or generate supervisory efficiencies in small bank supervision while maintaining safety and soundness. Exploring opportunities to aid community bankers in their implementation of CECL has been a priority for the group since its creation. Through significant effort and collaboration, the SBSWG and Federal Reserve Board staff developed the Scaled CECL Allowance for Losses Estimator (SCALE) method and tool to illustrate a simple and practical option that smaller community banks can use to estimate the allowances for credit losses (ACL) under CECL.

Federal Reserve staff presented the SCALE method and tool during an Ask the Fed webinar on July 15, 2021. The Financial Accounting Standards Board and the Conference of State Bank Supervisors also participated in the webinar.

The SCALE method is a simple, spreadsheet-based method developed to assist smaller community banks in calculating CECL-compliant ACL using proxy expected lifetime loss rates. Banks will still need to apply qualitative adjustments reflecting the bank's unique facts and circumstances. Bank management remains responsible for ensuring that the bank's allowances accurately reflect the credit risk in its portfolio and loss history. The SCALE method is one of many potentially acceptable CECL methods that a bank may use to estimate ACL. Further, the SCALE method is not a regulator-preferred method and does not ensure compliance with U.S. generally accepted accounting principles (GAAP) or any other regulatory requirement.

The SCALE tool is a template that community banks with total assets of less than $1 billion can use if they wish to use the SCALE method. This tool uses publicly available data from Schedule RI-C of the Call Report to derive the initial proxy expected lifetime loss rates. If a bank uses the SCALE tool, bank management must use judgment to further adjust the proxy expected lifetime loss rates. These adjustments should address bank-specific facts and circumstances to arrive at the final ACL estimate that adequately reflects a bank's loss history and the credit risk in its loan portfolios.

Governor Bowman says the SCALE tool supports efforts to appropriately tailor supervision and regulation for community banks. "The introduction of SCALE as a simple and practical way for smaller community banks to efficiently implement CECL should help to minimize the complications of CECL implementation and enable these institutions to remain focused on meeting the financial needs of their communities," she says. "I see the introduction of this tool as the beginning. We continue to look for other ways to assist banks in their efforts to implement CECL."

To access more information on the SCALE method and tool, visit www.supervisionoutreach.org/cecl/scale. The website includes a link to the archived Ask the Fed webinar that provides more details on the SCALE model and tool. The website also provides supporting materials, including the SCALE tool, tool instructions, and frequently asked questions. If you have questions about the SCALE method or tool, reach out to your local Reserve Bank contact.

CECL Practices at Regional Banks

As community banks continue to plan for CECL implementation, information from our 2020 offsite analysis of CECL practices at regional banking organizations (RBOs)[1] is being presented for consideration. The objective of this offsite analysis was to understand and document key processes, assumptions, and methodologies at regional banks that had implemented CECL in 2020 and to provide the status of implementation plans for those RBOs with a CECL implementation date after 2020. Examiners gathered information during regularly scheduled supervisory activities for 90 Federal Reserve–supervised RBOs.

Observations on CECL practices as of the third quarter of 2020 are summarized below. Practices at community banking organizations may differ from what is described

[1] A regional banking organization is defined as a bank or bank holding company with total assets between $10 billion and $100 billion that is supervised by the Federal Reserve.

below for regional banking organizations due to differences in risk exposures.

Most RBOs adopted CECL on January 1, 2020. Key implementation challenges noted by institutions included:

- incorporating pandemic economic considerations, including government support and loan forbearance programs, into the reasonable and supportable forecasts; and
- determining the effect of specific exposures (e.g., energy, hospitality, and retail credits).

On average, the immediate effect of CECL and the estimated measurement of lifetime losses on ACL was material, with an average increase in a bank's ACL balance of 48 percent. The banks' loan portfolio segments with the biggest change in ACL allocation after CECL implementation were commercial and industrial loans, commercial real estate loans, and one- to four-family residential loans.

RBOs primarily rely on the use of third-party service providers in the CECL process; however, institutions are largely leveraging their existing governance processes to oversee the CECL process. Most regional banks' CECL methodologies relied more on quantitative approaches, with 22 percent having an even balance between quantitative and qualitative approaches. All regional banks either have had an independent control review of CECL or plan to have one. For those institutions that will not implement CECL until 2023, implementation plans are generally on track. ■

Common Authentication Solution Adopted

LOGIN.GOV

The Federal Reserve and the other members of the Federal Financial Institutions Examination Council (FFIEC) recently completed a project that identified opportunities to reduce regulatory burden for community banks (i.e., supervised institutions with $10 billion or less in consolidated assets). One element of the project was resolving the differing and cumbersome authentication requirements that the FFIEC member agencies use to allow supervised institutions to access an agency's externally facing supervision systems.

As a result of this project, the FFIEC members adopted login.gov, a secure authentication solution that provides supervised institutions and FFIEC members with a single sign-on method for government websites, including access to their supervision systems. While login.gov can be used by all supervised institutions, it is especially helpful for smaller institutions. Users will now have a consistent and less confusing experience when they log in to the various FFIEC members' systems. Additionally, because the number of access methods will be reduced, users will not need to maintain multiple credentials to access different FFIEC members' systems, thereby creating a more seamless experience.

Login.gov, which is supported by the General Services Administration, adheres to the latest security standards established by security organizations such as the National Institute of Standards and Technology. Further, this single sign-on solution provides a high degree of security with privacy, multifactor authentication for access, and end-to-end encryption within the platform. In addition, login.gov allows organizational independence so that all FFIEC members may manage access to their own data.

FFIEC members will each establish their own implementation strategy and timeline for transitioning supervised institutions and their staff to login.gov. Therefore, supervised institutions should contact their primary regulator with any questions about login.gov and when they should use this new access platform.

FFIEC members will continue to evaluate opportunities to align their technological capabilities where possible to promote consistency among members and to reduce regulatory burden on supervised institutions. ■

A Message from Governor Bowman

Continued from page 3

just the incredible resilience of U.S. households and businesses but also very supportive monetary and fiscal policy. As a member of the FOMC, in my view, the most important challenge now is to ensure that our policy continues to be appropriately positioned to achieve our statutory goals of maximum employment and price stability.

With this challenge in mind, my FOMC colleagues and I have been discussing the impact of the Federal Reserve's asset purchases on the economy. Those purchases have played an important role in the Federal Reserve's response to the economic effects of the pandemic — by helping to support the flow of credit to U.S. households and businesses. But based on the progress we are seeing toward our policy goals, and assuming this progress continues, I believe it is appropriate to begin the process to scale back our asset purchases soon. Continuing these asset purchases seems unnecessary in light of the recovery to this point.

- On the price stability side of our mandate, as we have all seen, inflation has been running well above our 2 percent goal, and I suspect supply and demand imbalances are playing an important role in the rise in inflation this year. As the supply chain bottlenecks are worked out, these pressures will likely ease, but that could take some time, as some supply chain bottlenecks might continue well into 2022. Therefore, I am concerned that inflation could end up being higher than most expect. I will continue to closely monitor inflation pressures.
- On the maximum employment side of our mandate, economic conditions bode well for the achievement of our goal. I am watching labor force participation and employment as pandemic benefits programs end. As a result, I do expect to see more workers coming back into the labor force. I expect the unemployment rate to continue to decline, but at a slightly slower rate going forward.

During the pandemic, community banks were the lifeblood of many communities. Is the Federal Reserve doing anything to encourage community bank de novo applications?

Since joining the Federal Reserve Board, I have focused on reviewing the Federal Reserve's de novo supervisory program. Through this review, we found that de novo state member banks were subject to higher capital standards than state nonmember or national banks. In mid-2020, we addressed this disparity by revising the Fed's guidance on the supervision of de novo state member banks in Supervision and Regulation (SR) letter 20-16, "Supervision of De Novo State Member Banks," which in part provides for lower capital requirements and expanded exam frequencies for Fed member de novos.[5] We are also seeking ways to streamline the Federal Reserve's membership application process for both existing and de novo banks.

I have long been a strong proponent of additional research to identify the market constraints and regulatory barriers to bank formation. This type of research is necessary to lay the groundwork for future policy actions. We are also exploring ways to encourage the formation of new banks by providing technical assistance to prospective applicants. I also look forward to exploring other options to encourage new bank formation and will work with industry participants to advance this effort. ■

[5] SR letter 20-16 is available at www.federalreserve.gov/supervisionreg/srletters/SR2016.htm.

D.C. UPDATES

D.C. Updates features highlights of regulatory and policy actions taken by the Federal Reserve since the last issue as well as a listing of speeches and congressional testimonies of the Federal Reserve Board members that may be of interest to community bankers. For a list of Federal Reserve or interagency rulemakings and statements related to the pandemic, visit the Federal Reserve's COVID-19 Resources page, available at www.federalreserve.gov/covid-19.htm.

ACTIONS

Actions Related to Safety and Soundness Policy

Community Bank Guide for Conducting Due Diligence on Financial Technology Companies: On August 27, 2021, the federal bank regulatory agencies released a guide intended to help community banks assess risks when considering relationships with financial technology (fintech) companies. This guide covers six key areas of due diligence and highlights practical sources of information that may be useful when evaluating fintech companies. Supervision and Regulation (SR) letter 21-15/Consumer Affairs (CA) letter 21-11, "Guide for Community Banking Organizations Conducting Due Diligence on Financial Technology Companies," is available at www.federalreserve.gov/supervisionreg/srletters/sr2115.htm.

Proposed Risk Management Guidance for Third-Party Relationships: Federal bank regulatory agencies requested public comment on proposed guidance designed to help banking organizations manage risks associated with third-party relationships, including relationships with financial technology-focused entities. The July 13, 2021, press release is available at www.federalreserve.gov/newsevents/pressreleases/bcreg20210713a.htm.

Federal Reserve CECL Tool: On July 1, 2021, the Federal Reserve announced a new tool to help community banks implement the current expected credit losses (CECL) accounting standard. Known as the Scaled CECL Allowance for Losses Estimator (SCALE), the spreadsheet-based tool draws on publicly available regulatory and industry data to aid community banks with assets of less than $1 billion in calculating their CECL allowances. The Federal Reserve discussed the SCALE tool and answered questions during an Ask the Fed webinar on July 15, 2021. The session featured participation from the Financial Accounting Standards Board and the Conference of State Bank Supervisors. Webinar information is available at www.askthefed.org/. The SCALE tool is available at SupervisionOutreach.org/cecl. The July 1, 2021, press release is available at www.federalreserve.gov/newsevents/pressreleases/bcreg20210701a.htm.

FFIEC Architecture, Infrastructure, and Operations Examination Handbook: On June 30, 2021, the Federal Financial Institutions Examination Council (FFIEC) published the "Architecture, Infrastructure, and Operations" (AIO) booklet. The AIO booklet is one in a series of 11 booklets that make up the *FFIEC Information Technology Examination Handbook*. This handbook replaces the current "Operations" booklet published in July 2004. The new handbook focuses on enterprise-wide, process-oriented approaches that consider the design of technology within the overall business structure, implementation of IT infrastructure components, and delivery of services and value for customers. SR letter 21-11, "FFIEC Architecture, Infrastructure, and Operations Examination Handbook," is available at www.federalreserve.gov/supervisionreg/srletters/SR2111.htm.

Interagency Statement on the Anti-Money Laundering/Countering the Financing of Terrorism National Priorities: On June 30, 2021, federal and state regulatory agencies issued an interagency statement on the Anti-Money Laundering/Countering the Financing of Terrorism National Priorities (AML/CFT Priorities). The intent of this interagency statement is to provide clarity on the AML/CFT Priorities. SR letter 21-10, "Interagency Statement on the Issuance of the Anti-Money Laundering/Countering the Financing of Terrorism National Priorities," is available at www.federalreserve.gov/supervisionreg/srletters/SR2110.htm.

***Bank Secrecy Act/Anti-Money Laundering Examination Manual* Update:** On June 22, 2021, members of the FFIEC released several updated sections and related examination procedures to the *Bank Secrecy Act/Anti-Money Laundering Examination Manual*. The revised sections included:

- Purchase and Sale of Monetary Instruments Recordkeeping
- Special Measures
- Reports of Foreign Financial Accounts
- International Transportation of Currency or Monetary Instruments Recordkeeping

SR letter 21-09, "Release of Updated Sections of the Federal Financial Institutions Examination Council's *Bank Secrecy Act/Anti-Money Laundering Examination Manual*," is available at www.federalreserve.gov/supervisionreg/srletters/SR2109.htm.

Actions Related to Consumer Policy

Community Reinvestment Act Modernization: The Federal Reserve Board announced that it is committed to working with the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation to jointly strengthen and modernize regulations implementing the Community Reinvestment Act. The July 20, 2021, press release is available at www.federalreserve.gov/newsevents/pressreleases/bcreg20210720b.htm.

CRA Consideration for Community Development Activities in Puerto Rico and the U.S. Virgin Islands in Response to Hurricane Maria Extension: On May 27, 2021, CA letter 21-9, "Extension of CRA Consideration for Community Development Activities in Puerto Rico and the U.S. Virgin Islands in Response to Hurricane Maria," was issued to extend the period for Community Reinvestment Act (CRA) consideration of community development activities that help to revitalize or stabilize Puerto Rico and the U.S. Virgin Islands related to Hurricane Maria. The CA letter is available at www.federalreserve.gov/supervisionreg/caletters/caltr2109.htm.

Home Mortgage Disclosure Act Quarterly Reporting Resumes: On May 14, 2021, CA letter 21-8, "Resumption of Home Mortgage Disclosure Act (HMDA) Quarterly Reporting," was issued to instruct all financial institutions required to report quarterly to do so, beginning with their 2021 first-quarter data. The CA letter is available at www.federalreserve.gov/supervisionreg/caletters/caltr2108.htm.

Other Board Actions and Releases

Amendments to Regulation D: The Federal Reserve Board announced the approval of a final rule amending Regulation D to eliminate references to an interest on required reserves rate and to an interest on excess reserves rate and replace them with a single interest on reserve balances rate. The final rule also simplifies the formula used to calculate the amount of interest to be paid on such balances and makes other minor conforming amendments. The final rule became effective on July 29, 2021. The June 2, 2021, press release is available at www.federalreserve.gov/newsevents/pressreleases/bcreg20210602a.htm.

Technological Advances in the Global Payments Landscape: Federal Reserve Chair Jerome H. Powell outlined the Federal Reserve's response to technological advances driving rapid change in the global payments landscape. The Federal Reserve is studying these developments and exploring ways that it might refine its role as a core payment services provider and as the issuing authority for U.S. currency. The May 20, 2021, press release, including a video message from Chair Powell, is available at www.federalreserve.gov/newsevents/pressreleases/other20210520b.htm.

SPEECHES

Speeches Related to the U.S. Economy and Monetary Policy

Vice Chair for Supervision Randal K. Quarles gave a speech at the Venice International Conference on Climate Change, Venice, Italy, on July 11, 2021. His speech, titled "Disclosures and Data: Building Strong Foundations for Addressing Climate-Related Financial Risks," is available at www.federalreserve.gov/newsevents/speech/quarles20210711a.htm.

Governor Michelle W. Bowman gave a speech at the Policy Summit 2021: Pathways to Economic Resilience in our Communities, Federal Reserve Bank of Cleveland, Cleveland, OH, (via prerecorded video) on June 23, 2021. Her speech, titled "Building Economic Resilience in Communities," is available at www.federalreserve.gov/newsevents/speech/bowman20210623a.htm.

Governor Lael Brainard gave a speech at the Economic Club of New York, New York, (via webcast) on June 1, 2021. Her speech, titled "Remaining Steady as the Economy Reopens," is available at www.federalreserve.gov/newsevents/speech/brainard20210601a.htm.

Vice Chair for Supervision Randal K. Quarles gave a speech at the Hutchins Center on Fiscal and Monetary Policy, The Brookings Institution, Washington, D.C., (via prerecorded video) on May 26, 2021. His speech, titled "The Economic Outlook and Monetary Policy," is available at www.federalreserve.gov/newsevents/speech/quarles20210526b.htm.

Vice Chair for Supervision Randal K. Quarles gave remarks at the National Association of Insurance Commissioners International Insurance Forum (via prerecorded video) on May 26, 2021. His remarks are available at www.federalreserve.gov/newsevents/speech/quarles20210526a.htm.

Vice Chair Richard H. Clarida gave remarks at Fostering a Resilient Economy and Financial System: The Role of Central Banks 25th Annual Financial Markets Conference, sponsored by the Center for Financial Innovation and Stability, Federal Reserve Bank of Atlanta, Amelia Island, FL, (via webcast) on May 17, 2021. His remarks, titled "Sovereign Markets, Global Factors," are available at www.federalreserve.gov/newsevents/speech/clarida20210517a.htm.

Governor Christopher J. Waller gave a speech at the Global Interdependence Center's 39th Annual Monetary and Trade Conference, The LeBow College of Business, Drexel University, Philadelphia, (via webcast) on May 13, 2021. His speech, titled "The Economic Outlook and Monetary Policy," is available at www.federalreserve.gov/newsevents/speech/waller20210513a.htm.

Vice Chair Richard H. Clarida gave a speech at the NABE International Symposium: A Vision of the Economy Post COVID, Washington, D.C., (via webcast) on May 12, 2021. His speech, titled "U.S. Economic Outlook and Monetary Policy," is available at www.federalreserve.gov/newsevents/speech/clarida20210512a.htm.

Governor Lael Brainard gave a speech at The Road to Recovery and What's Next, a virtual conference sponsored by the Society for Advancing Business Editing and Writing (via webcast) on May 11, 2021. Her speech, titled "Patience and Progress as the Economy Reopens and Recovers," is available at www.federalreserve.gov/newsevents/speech/brainard20210511a.htm.

Governor Michelle W. Bowman gave a speech at the Colorado Forum, Denver, (via webcast) on May 5, 2021. Her speech, titled "The Economic Outlook and Implications for Monetary Policy," is available at www.federalreserve.gov/newsevents/speech/bowman20210505a.htm.

Chair Jerome H. Powell gave remarks at the 2021 Just Economy Conference sponsored by the National Community Reinvestment Coalition, Washington, D.C., (via webcast) on May 3, 2021. His remarks are available at www.federalreserve.gov/newsevents/speech/powell20210503a.htm.

Speeches Related to Supervision and Regulation

Vice Chair for Supervision Randal K. Quarles gave a speech at the Prudential Regulation Conference (via webcast) on June 3, 2021. His speech, titled "Jet Flight, Mail Bags, and Banking Regulation," is available at www.federalreserve.gov/newsevents/speech/quarles20210603a.htm.

Speeches Related to Payment Systems

Vice Chair for Supervision Randal K. Quarles gave a speech at the 113th Annual Utah Bankers Association Convention, Sun Valley, ID, on June 28, 2021. His speech, titled "Parachute Pants and Central Bank Money," is available at www.federalreserve.gov/newsevents/speech/quarles20210628a.htm.

Governor Lael Brainard gave a speech at the Consensus by CoinDesk 2021 Conference, Washington, D.C., (via webcast) on May 24, 2021. Her speech, titled "Private Money and Central Bank Money as Payments Go Digital: An Update on CBDCs," is available at www.federalreserve.gov/newsevents/speech/brainard20210524a.htm.

TESTIMONIES

Chair Jerome H. Powell testified on the Semiannual Monetary Policy Report to the Congress before the Committee on Financial Services, U.S. House of Representatives, Washington, D.C., on July 14, 2021. Chair Powell submitted identical remarks to the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, in Washington, D.C., on July 15, 2021. The testimony is available at www.federalreserve.gov/newsevents/testimony/powell20210714a.htm.

Chair Jerome H. Powell testified on the Federal Reserve's Response to the Coronavirus Pandemic before the Select Subcommittee on the Coronavirus Crisis, U.S. House of Representatives, Washington, D.C., on June 22, 2021. The testimony is available at www.federalreserve.gov/newsevents/testimony/powell20210622a.htm.

Tips to Protect Against Cybersecurity Breaches

by Nancy Hunter, Vice President, Information Technology Services, Federal Reserve Bank of Philadelphia

In newspapers, on television, or in banking magazines, it is hard to escape the topic of cybersecurity. It feels like it is talked about everywhere. In the past year, cyber incidents have impacted many in unexpected ways: higher gas prices because of the Colonial pipeline ransomware attack, concern about food supply disruptions related to the cyber breach of JBS Meats, a surge in unemployment fraud, criminals impacting the IT infrastructure with the SolarWinds hack, and an increase in cyber theft at ATMs. These types of crimes have been occurring for many years, but the difference is that now they seem to be more public, and the overall impacts are greater.

How can businesses and individuals better protect themselves? Here are some action steps to take:

- Patch the software in use at home and at work. Criminals know what vulnerabilities exist and when software patches are not applied. They exploit them regularly.
- Practice good password hygiene. Make sure passwords are complex and updated frequently. Do not reuse the same passwords for different systems. Criminals will try passwords that were hacked through published breaches on different systems years later. Be more creative than using a child's or pet's name as a password. Try using phrases that are easy to remember as a password. For example, use IloveMyFIDO!9751 instead of FIDO123.
- Thwart phishing attacks by not clicking on links from unfamiliar sources. Businesses should conduct phishing tests for everyone, even the leadership.
- Prepare before a possible attack. Practice possible cyberattack scenarios through tabletop events so that muscle memory will assist response in the event of an actual attack.
- Build relationships now with local law enforcement and the FBI so they are better able to help when needed.

It is always the right time to do the right thing in order to be safe.

Scan with your smartphone or tablet to access Community Banking Connections online.