FEDERAL RESERVE SYSTEM

SPECIAL ISSUE: CYBERSECURITY

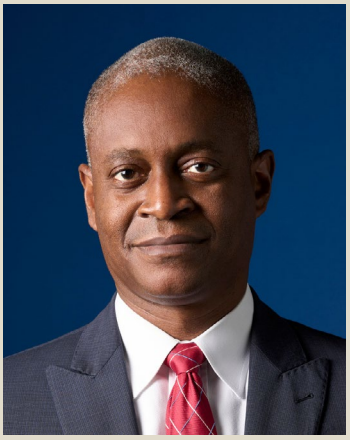
COMMUNITY BANKING
CONNECTIONS®

A SUPERVISION AND REGULATION PUBLICATION

Third Issue 2022

Technology and Innovation in Community Banking: Opportunities, Challenges, and the Fed

by Raphael W. Bostic, President and Chief Executive Officer, Federal Reserve Bank of Atlanta



Raphael W. Bostic

Community banks are beset by challenges on numerous fronts. Foremost among them is the relentless advance of technology and, along with it, heightened customer expectations for convenience and instantaneous service.

At a time when consumers and business customers can readily turn to digital offerings for all manner of financial services, traditional financial institutions must keep pace to remain relevant. This can be particularly tough for community banks, which typically face resource constraints — human, financial, and otherwise. As a result, meeting customer demands for technology-enabled services often means seeking help from partners. Partnerships with third-party firms can entail supplying services such as mobile banking directly to customers or, in some cases, offering services inside a physical branch.

Often these service providers are financial technology companies, or fintechs. These sorts of companies normally have roots in the information technology industry and thus may not instinctively understand the regulatory and fiduciary obligations that are second nature to banks.

In this space, I would like to share a few thoughts on the Federal Reserve's role in helping community banks address both the opportunities and the challenges that technology and innovation present. In particular, I will discuss third-party partnerships because they are especially important for community banks in today's financial services marketplace.

Facilitating Community Bank Engagement with Innovation

What role can the Fed play as community banks seek to navigate this new and challenging competitive landscape? Most important, in our capacity as a safety-and-soundness supervisor, we are committed to helping community banks pursue technology innovation, and thus engage with service providers, in a safe, sound, and responsible manner.

In my view, this work dovetails perfectly with our Reserve Bank's strategic priority to build an economy that works

for everyone by promoting economic mobility and resilience because community banks are pillars of our local economies.

Let me mention an example. Just before the pandemic, the Federal Reserve Bank of Atlanta hosted an event that the Federal Reserve System calls *Innovation Office Hours*. We connected two dozen Sixth District fintech entrepreneurs and bankers with experts from the Atlanta Fed and the Federal Reserve Board to discuss payments security, regulation, financial inclusion, and other relevant matters. The fundamental aim of outreach like this is to influence the direction of innovation so that fintech firms are more likely to incorporate security, sound risk management, and financial inclusion into their development processes. Innovation is essential to a healthy financial system, but we want innovators to think about risk in a very fundamental way.

Likewise, we want community bankers to understand both the opportunities and the risks inherent in engaging with third-party service providers that are often very different culturally from financial institutions. To that end, we have taken numerous steps to help community banks navigate the complexities of third-party partnerships.

In 2021, the Federal Reserve Board, along with the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation, proposed guidance to help banking organizations manage risks associated with third-party relationships.[1]

The three federal financial regulatory agencies also published a guide to assist community banks in conducting due diligence on fintech firms.[2] Seeking a partnership with a newer fintech company — and many are relatively new — may introduce particular complications. For example, a less experienced technology partner may offer a suitable product but may not understand the bank's regulatory obligations or have fully developed operational or compliance frameworks. To help address concerns of this nature, the Federal Reserve

[1] See "Proposed Interagency Guidance on Third-Party *Relat*ionships: Risk Management," available at www.federalreserve.gov/newsevents/pressreleases/files/bcreg20210907a1.pdf.

[2] See *Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks,* available at www.federalreserve.gov/publications/conducting-due-diligence-on-financial-technology-firms.htm.

Community Banking Connections (CBC) is distributed to institutions supervised by the Federal Reserve System. Current and past issues of *CBC* 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 phone at 800-372-0248.

Editor: **Hilda Guay** Assistant Editor: **Maura Fernbacher**
Project Manager: **Ivy Washington** Designer: **Monica Conrad** Web Architect: **Christopher Pascual**

> Innovation is essential to a healthy financial system, but we want innovators to think about risk in a very fundamental way.

published a paper in September 2021 on the evolving dynamics of community bank–fintech partnerships.[3]

Built around insights from bankers, fintechs, and other stakeholders, the paper outlines the strategic and tactical decisions that support effective partnerships. Notably, the paper makes clear that a community bank's strategic goals and those of its fintech partners should align and that banks need to embrace a culture of ongoing innovation.

Ultimately, it is the banks' responsibility to ensure that outsourced activities are carried out safely and soundly. So, to form fruitful partnerships, bankers need to clearly understand the potential pitfalls upfront.

For many community banks, significant service providers (SSPs) will be the conduit through which technology and innovation are introduced. Thus, it will be important for community banks to be aware of the strength and health of SSPs. The Federal Reserve and other federal financial regulatory agencies exercise regulatory oversight of SSPs. One important focus of our SSP supervision is information security. As one example of how seriously we take this issue, the Federal Reserve System is hiring more than two dozen cybersecurity specialists to help ensure that service providers deploy sound cyber defense technologies, staff, and practices.

[3] See *Community Bank Access to Innovation Through Partnerships*, available at www.federalreserve.gov/publications/files/community-bank-access-to-innovation-through-partnerships-202109.pdf.

Based on their SSP supervision activities, the agencies issue regular examination reports on the condition of service providers, which are broadly similar to an exam report for financial institutions. Therefore, I suggest that community bankers review reports on the significant service providers with which they have contractual relationships. These examination reports provide valuable information for a bank in monitoring its service providers and can be requested from the bank's primary federal regulator.

Honing Our Analytics Capabilities to Help Community Banks

Applications of technology and innovation are not limited to customer-facing interactions. We in the Federal Reserve System are also embracing the use of new tools and techniques to supervise and engage with community banks. We have long been working to reduce regulatory burden, and we continually refine our regulatory approach and tailor our supervision to the size and complexity of institutions. Technology has played an important role in advancing the efficiency and effectiveness of our supervisory process. A good example of this is that we use technological tools to conduct significant portions of our examinations remotely, from our offices, something that we started before the pandemic.

Another way the Atlanta Fed is doing this is by honing our data analytics capabilities, something our peer Reserve Banks are also pursuing. In our efforts to assess potential risk and thus target our supervisory efforts appropriately, we analyze numerous data streams, including commercial real estate metrics, residential housing metrics, and commercial risk scores from leading data providers such as CoStar. We also employ a variety of analytical tools and modeling techniques, including open-source tools such as R Programming and data visualization software such as Tableau and PowerBI.

We also build analytical tools that community bankers can use. To cite a couple of examples, one of our economists developed the GDPNow tool, which synthesizes a great deal of data to estimate coming

quarters' gross domestic product growth.[4] GDPNow is publicly available for anyone to better understand macroeconomic currents. Additional macroeconomic Atlanta Fed tools offer insights on inflation, labor markets, and more.[5] Further, analysts in our Supervision, Regulation, and Credit division built data analytics engines that track home affordability — the Home Ownership Affordability Monitor[6] — and commercial real estate conditions — the Commercial Real Estate Momentum Index.[7]

These tools represent an important aspect of our work beyond traditional monetary policy and financial supervision. Through these tools, all of which are available on our website, we provide expertise, evidence-based research, and analytics to help community banks as well as nonprofits, local governments, and community organizations fortify economic growth and the mobility and resilience of the families they serve and the communities in which they operate.

Atlanta Fed President Raphael Bostic speaks to a reporter in Atlanta regarding COVID-19 and its impact.

Our Economy Needs Community Banks

There is no doubt that community banks are essential institutions in so many of our towns and cities across this country. These institutions often know customers better than a larger bank might, which can be critical for expanding access to banking services in rural, urban, and underserved communities. And while many consumers and businesses have an array of financial services options, community banks are important providers of key services to niche populations and business sectors.

In cities, community banks, including minority-owned institutions, support businesses and households that may not be a focus of larger institutions. Community banks are flexible for business loans and nimble with loan requests.

Indeed, community banks account for an outsize share of loans to important sectors, including commercial real estate, small business, and agriculture, according to the FDIC's *2020 Community Banking Study*.[8]

Even as we wrestle with elevated inflation and uncertainty across the global economy, the Federal Reserve is paying close attention to community banks. These institutions face numerous challenges, but the industry and regulatory agencies can and must devise creative ways to support them. In particular, the agencies need to continue to support community bankers in their efforts to incorporate the latest technology into their products and services. Community banks bring unique economic benefits to the communities where they operate. Those communities and our economy need them. ■

[4] More information about GDPNow is available at www.atlantafed.org/cqer/research/gdpnow.aspx.

[5] The tools are available at www.atlantafed.org/research/data-and-tools.aspx.

[6] The Home Ownership Affordability Monitor is available at www.atlantafed.org/center-for-housing-and-policy/data-and-tools/home-ownership-affordability-monitor.aspx.

[7] The Commercial Real Estate Momentum Index is available at www.atlantafed.org/center-for-housing-and-policy/data-and-tools/commercial-real-estate-momentum-index.aspx.

[8] The study is available at www.fdic.gov/resources/community-banking/report/2020/2020-cbi-study-full.pdf.

Recent Trends in Ransomware

by Chad Siegrist, Assistant Vice President, Supervision and Regulation, and Cybersecurity Analytic Support Team, Federal Reserve Bank of Cleveland, and Jason Tarnowski, Vice President, Supervision and Regulation, and Cybersecurity Analytic Support Team, Federal Reserve Bank of Cleveland

Ransomware attacks target all industries and frequently result in direct and indirect financial losses, operational disruptions, and customer reputation consequences. In May 2021, ransomware groups attacked at least three U.S. community banks.[1] However, the most notorious ransomware event in May 2021 was launched by the DarkSide (aka BlackMatter) ransomware group, which attacked Colonial Pipeline, a large oil and gas pipeline that serves the southeastern United States. The attack impacted the company's billing system, but the firm shut down the pipeline until it could determine that the attackers hadn't damaged or gained access to critical safety and control systems. The attack resulted in weeklong fuel shortages for large areas in the eastern and southeastern United States. Colonial Pipeline quickly paid the attackers nearly $5 million in bitcoins, but it still took several days for Colonial's systems to be restored. While Colonial Pipeline's incident captivated the media about the risk ransomware attacks pose to critical energy infrastructure, the financial sector is also at serious risk.

Although it is difficult to measure the total impact and financial losses resulting from ransomware attacks, the U.S. Department of the Treasury reports the dollar amount of global suspected ransomware payments between January and June 2021 exceeded that during all of 2020.[2] Specific to the banking industry, one security firm reported a 1,318 percent increase in ransomware attacks targeting the financial sector during the first half of the year.[3]

Ransomware Impact on Community Banks

Since May 2021, at least seven community banks in California, Florida, Illinois, Kansas, Michigan, and Minnesota have become the targets of ransomware attacks, according to dark web blogs belonging to ransomware groups. Typically, these groups do not release information about affected organizations for several days to allow for initial negotiations, which suggests that the total number of community banks affected is likely far higher.

> "Ransomware attackers continue to increase the sophistication of their operations."

In August 2021, the AvosLocker ransomware group attacked a California community bank. In addition to encrypting and locking the bank's computer systems, the attackers stole sensitive customer information, including names, addresses, Social Security numbers, tax forms, and loan documents. The bank notified its customers of the breach and offered credit monitoring services for the impacted customers, adding to the financial, operational, and reputational costs of the attack.[4]

Typical Ransomware Attack Cycle

While ransomware attacks can use different tools, methods, and timing to compromise systems, there are common steps involved, as depicted in the Figure. These

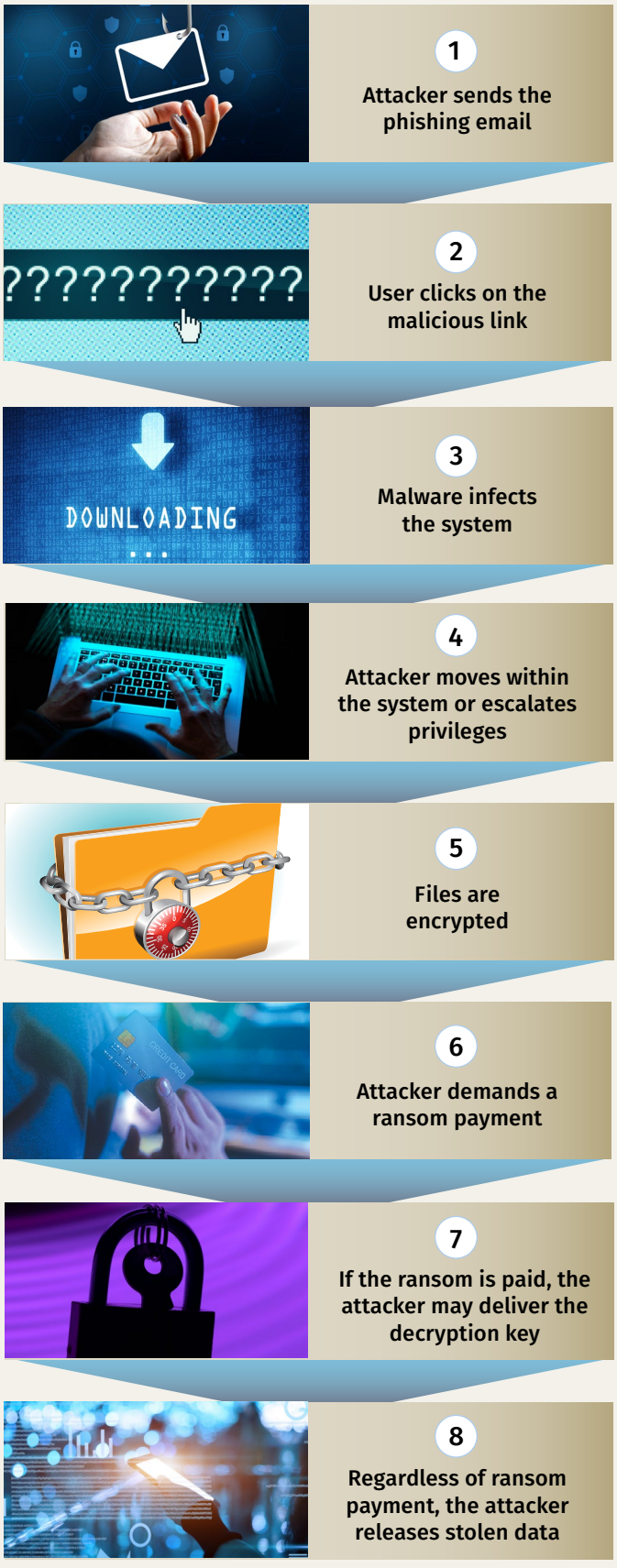
[1] See Penny Crosman, "'It's Very Scary': Small Banks Quietly Hit by Ransomware Attacks," *American Banker*, May 24, 2021, available at www.americanbanker.com/news/its-very-scary-small-banks-quietly-hit-by-ransomware-attacks.

[2] See "Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021," U.S. Treasury Financial Crimes Enforcement Network report, October 1, 2021, available at www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf.

[3] See "Attacks Surge in 1H 2021 as Trend Micro Blocks 41 Billion Cyber Threats," Trend Micro, September 14, 2021, available at https://newsroom.trendmicro.com/2021-09-14-Attacks-Surge-in-1H-2021-as-Trend-Micro-Blocks-41-Billion-Cyber-Threats.

[4] See Bill Toulas, "Pacific City Bank Discloses Ransomware Attack Claimed by AvosLocker," *Bleeping Computer*, October 11, 2021, available at www.bleepingcomputer.com/news/security/pacific-city-bank-discloses-ransomware-attack-claimed-by-avoslocker/.

Figure: Typical Ransomware Attack Sequence



steps can occur over several months or in just a few minutes. Knowing how to detect and respond to each step is critical in planning response procedures and implementing effective controls, especially before the data encryption step.

Evolving Ransomware Tactics

Ransomware attackers continue to increase the sophistication of their operations. For example, ransomware groups sometimes outsource initial access and persistence steps to other "initial access brokers." Initial access brokers specialize in gaining access to targeted organizations' networks that the ransomware attackers then use to start the reconnaissance and encryption steps of the ransomware attack. Some ransomware groups have even established dedicated "customer support" centers to communicate with their victims, negotiate a ransom price, and explain the details of making cryptocurrency-based ransom payments.[5]

Ransomware attackers are also increasing their use of "double extortion attacks," in which attackers threaten to leak stolen data if victims fail to pay the ransom. This tactic allows attackers to pressure victims to pay a ransom even if the affected organization can restore its systems from unaffected backups.

The Table shows the financial losses and operation disruption durations experienced by customers of Coveware, a ransomware mitigation company, because of ransomware attacks.

Incident Reporting

Given the potential impact that cyber incidents, including ransomware, may have on the financial sector, the federal banking agencies approved a final rule[6] to improve the reporting and sharing of information. The final rule, which became effective May 1, 2022, requires a banking organization to notify its federal regulator of any significant computer-security incident within 36 hours. Community

[5] See Joe Tidy, "How Hackers Extorted $1.14m from University of California, San Francisco," BBC.com, June 29, 2020, available at www.bbc.com/news/technology-53214783.

[6] See "Agencies Approve Final Rule Requiring Computer-Security Incident Notification," available at www.federalreserve.gov/newsevents/pressreleases/bcreg20211118a.htm.

Resources and Guidance

Cybersecurity and Infrastructure Security Agency

The agency offers resources on its ransomware-focused website, www.cisa.gov/stopransomware, including:

- A response checklist, www.cisa.gov/stopransomware/ransomware-guide
- Prevention best practices, www.cisa.gov/stopransomware/how-can-i-protect-against-ransomware
- A list of bad practices, www.cisa.gov/stopransomware/bad-practices

Federal Bureau of Investigation

The FBI has two relevant sites:

- https://ransomware.ic3.gov/default.aspx, to report ransomware incidents and ransom payments made
- www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware, detailing best practices for ransomware prevention

Federal Financial Institutions Examination Council (FFIEC)

The FFIEC's cybersecurity awareness page, www.ffiec.gov/cybersecurity.htm, includes:

- A cybersecurity assessment tool, www.ffiec.gov/cyberassessmenttool.htm
- A cybersecurity resource guide for financial institutions, www.ffiec.gov/press/pdf/FFIEC%20Cybersecurity%20Resource%20Guide%20for%20Financial%20Institutions.pdf
- A statement on cyberattacks involving extortion, www.ffiec.gov/press/PDF/FFIEC%20Joint%20Statement%20Cyber%20Attacks%20Involving%20Extortion.pdf

Financial Services Information Sharing and Analysis Center

The center is an excellent resource for community banks to raise awareness and understanding of current threats, including indicators of compromise to help firms identify potential attacks on their infrastructure. See its website at www.fsisac.com.

"Sound Practices to Strengthen Operational Resilience"

This joint paper by the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation has guidance applicable to community banks. The paper is available at www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201030a1.pdf.

Table: Ransomware Trends

	1Q21	2Q21	3Q21	4Q21
Average Ransom Payment ($)	220,298	136,576	139,739	322,168
Average Days of Downtime (Incident Duration and Business Disruption)	23	23	22	20
Financial Services Industry as a Percent of All Ransomware Attacks	4.4%	6.6%	4.9%	6.6%
Companies with <1,000 Employees as a Percent of All Attacks	68.1%	69.2%	83.7%	81.6%

Sources: Coveware.com: "Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound," April 29, 2021, available at www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound; "Q2 Ransom Payment Amounts Decline as Ransomware Becomes a National Security Priority," July 23, 2021, available at www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority; "Ransomware Attackers Down Shift to 'Mid-Game' Hunting in Q3 2021," October 21, 2021, available at www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts; and "Law Enforcement Pressure Forces Ransomware Groups to Refine Tactics in Q4 2021," available at www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021

banks should review the final rule and take the necessary steps to comply with the requirements in the regulation.

Additionally, community banks that have an established relationship with or services provided by the Federal Reserve's Financial Services (e.g., FedWire, FedLine Advantage) should be familiar with the reporting requirements under Operating Circular No. 5.[7] Prompt reporting of cyber incidents will help to minimize any disruption of services and maintain the integrity of these systems.

Ransomware Outlook for 2022

Ransomware attackers are increasingly targeting small and medium-size businesses, which includes community banks. For the third quarter of 2021, a security firm specializing in ransomware mitigation reported a 14.5 percent increase in the number of attacks targeting organizations with fewer than 1,000 employees.[8] Attackers may be focusing on smaller organizations because they have limited information technology and cybersecurity resources to detect and respond to cyberattacks. Attackers may also be wary of targeting large critical infrastructure institutions following the Colonial Pipeline attack, as the United States and other countries have taken swift law enforcement actions against ransomware groups attacking critical infrastructure institutions. ■

[7] "Federal Reserve Banks Operating Circular No. 5" is available at www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/063021-operating-circular-5.pdf.

[8] See "Ransomware Attackers Down Shift to 'Mid-Game' Hunting in Q3 2021," Coveware.com, October 21, 2021, available at www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts.

Ransomware Defense: A Discussion with the Regulators

by Ray Bolton, CRSB Examiner, Supervision and Regulation, Federal Reserve Bank of Chicago; Chad Siegrist, Assistant Vice President, Supervision and Regulation, and Cybersecurity Analytic Support Team, Federal Reserve Bank of Cleveland; and Jason Tarnowski, Vice President, Supervision and Regulation, and Cybersecurity Analytic Support Team, Federal Reserve Bank of Cleveland

Ransomware is a type of malicious software that encrypts data, making it difficult for the owner of the data to access or recover. Attackers demand a ransom to decrypt the data. Ransomware is one of the fastest-growing cyber risks faced by banks, and cyberattackers' methods and tactics are constantly evolving. Community banks need to remain vigilant in understanding how their systems could be compromised and what controls and procedures are needed to effectively protect against and recover from an attack. Community banks should take steps to discuss and prepare for the eventuality of a ransomware attack that disrupts services as well as renders critical data unusable.

Industry Practices

The following are common industry practices to help banks defend against ransomware attacks. These practices are consistent with Federal Financial Institutions Examination Council (FFIEC) Information Security guidance.[1]

1. **Risk Management** — A bank's board of directors and management should investigate and assess the bank's risk exposure to ransomware attacks, regularly assess and test controls against ransomware attack scenarios, and support the prompt remediation of any control issues identified.

2. **Awareness** — All bank personnel should be made aware of the risk that ransomware poses to the bank and be trained on how to identify and report potential ransomware attempts.

3. **Inventory and Vulnerability Management** — A bank should have processes in place to maintain an accurate and timely inventory of hardware, software, connections, and data assets and have programs in place that identify vulnerabilities in its operating environment. Processes should also be in place to track patching of a bank's various banking systems and applications to address any potential vulnerabilities and document risk acceptance of unremediated vulnerabilities.[2,3]

4. **Backup Architecture** — Backup operations should be designed to protect backed-up data from threat actors. Air-gapped[4] backups, utilizing write once, read many (WORM)[5] technology, or other vendor-specific architectures are potential options to implement.

5. **Configuration Management** — Information systems should have consistent baseline configurations, including "hardening"[6] requirements, applied throughout their life cycles.[7] Hardening requirements should incorporate vendor documentation and industry best practices for specific technologies. Organizations

[1] *FFIEC IT Handbook InfoBase,* available at https://ithandbook.ffiec.gov/.

[2] *FFIEC Information Technology Examination Handbook, Information Security,* "II.A.2 Vulnerabilities," September 2016, available at https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iia-risk-identification/iia2-vulnerabilities.aspx.

[3] *FFIEC Information Technology Examination Handbook, Information Security,* "IV.A.2(c) Vulnerability Assessments," September 2016, available at https://ithandbook.ffiec.gov/it-booklets/information-security/iv-information-security-program-effectiveness/iva-assurance-and-testing/iva2-types-of-tests-and-evaluations/iva2(c)-vulnerability-assessments.aspx.

[4] An air gap is a security measure in which a copy of the backup is stored off the network in a completely separate physical location in order to allow the bank to restore data quickly in the event the network backups are compromised.

[5] WORM is a data storage technology that allows data to be written to a storage medium only once but read many times. This prevents the data from being erased or modified.

[6] In computer security, *hardening* refers to the process of reducing the available ways of attack, or surface of vulnerability. Common examples are changing default passwords and removing unnecessary software.

[7] *FFIEC Information Technology Examination Handbook, Information Security,* "II.C.10 Change Management Within the IT Environment," September 2016, available at https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic10-change-management-within-the-it-environment.aspx.

should consistently manage changes affecting baseline configuration, which involves a security impact analysis to determine whether any residual changes to the attack surface put the organization at risk.

6. **Network Segmentation** — To limit threat actor movement in the event that an intruder has established a foothold in a bank's system, a bank should segment networks by functionality, sensitivity, or another relevant attribute.[8] A zero-trust system in which data and resources are inaccessible by default and require user identity verification for each connection is one option.

7. **Third-Party Risk Management** — Banking organizations should identify risks associated with third-party relationships. A bank should dictate to a third party the bank's expectations for preventing ransomware incidents and for reporting any potential ransomware attacks. Secure architecture should prevent ransomware from spreading into an environment from a third party.[9]

8. **Email-Based Protections** — A bank's email filtering process should identify and prevent malicious messages, especially those that may contain ransomware attack tools, from reaching end users.

While not exhaustive, these practices will help prepare for and reduce the impact of a ransomware event. However, no single practice or even set of practices can completely eliminate the risk and impact of a ransomware attack on a bank.

[8] *FFIEC Information Technology Examination Handbook, Information Security,* "II.C.9 Network Controls," September 2016, available at https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic9-network-controls.aspx.

[9] *FFIEC Information Technology Examination Handbook, Information Security,* "II.C.20 – Oversight of Third-Party Service Providers," September 2016, available at https://ithandbook.ffiec.gov/it-booklets/information-security/ii-information-security-program-management/iic-risk-mitigation/iic20-oversight-of-third-party-service-providers.aspx.

Information Technology (IT) Experts' Perspectives

Several ransomware experts from the Federal Reserve Bank of Chicago were interviewed for this article — Colin Gavin, lead risk management specialist in System Cyber, Anthony Toins, senior CRSB examiner and IT risk specialist, and Ahmed Hussain, risk management specialist on the Service Provider Team. These experts provided their thoughts on industry practices and additional insight on ransomware from a regulatory perspective.

The industry practices that are outlined earlier are great ways for banks to reduce their risk and better prepare for a ransomware attack. What else can banks do?

Anthony: Despite the efforts of institutions to protect their networks, banks should assume that an attacker will penetrate their defenses. Threat actors are constantly changing their attack vectors and evolving their tactics and tools due to new vulnerabilities. Every institution should have a formal comprehensive incident plan, or a more specific ransomware playbook, to follow when an attacker is able to access its network. This includes steps bank management should follow with a managed security service provider (MSSP) and other third-party service providers (TSPs). Institutions should periodically test the plan and playbook with all relevant parties and share any lessons learned.

Colin: That's a great point, Anthony, and as with any adverse situation that may negatively affect an organization, the ability to quickly return to normal is paramount. You have to be able to develop a path to normalcy that is proven and fits within the stated service-level agreements with your MSSP or TSP. If a bank does not have that type of mechanism in place, then I would recommend that it close this gap by developing backup or even isolation tactics if a particular endpoint starts transmitting known malicious signatures to other devices. You may adopt a proactive stance to block that system from the network until a proper investigation can be conducted.

Meet the Experts:

Colin Gavin

Lead Risk Management Specialist in System Cyber

Anthony Toins

Senior CRSB Examiner and IT Risk Specialist

Ahmed Hussain

Risk Management Specialist on the Service Provider Team

Ahmed: Very true. Another growing ransomware risk area has been the proliferation of bank-owned mobile devices. Community bank executives are often provided with bank-owned mobile devices for various work-related activities and communications in which text-messaging features are employed. Now that users are more educated about email phishing, threat actors are using text-messaging to route ransomware into devices, as people tend to be less cognizant of the dangers on their mobile phones than on their computers. With the sudden rise of the remote work environment, threat actors are targeting mobile devices of bank employees, as these devices are often separated from the corporate network. I suggest managers at community banks employ strict security controls on these bank-issued mobile devices, for example, lists of banned applications, download blocking, and feature controls including remote device lock, erasure, port control, and camera and video access.

How would you say preparing for or mitigating ransomware risk is different for community banks compared with larger institutions?

Colin: I think it really depends on the bank's strategy. A proactive approach for training and preparing staff for when an attack hits — and not if an attack will take place — will always be the preferential option. The goal remains the same if you are a community banking organization versus a large or foreign banking organization. How quickly can you return to normal? Everyone in the organization should be trained on what to do before and after an attack takes place. Tabletop exercises should be conducted to identify and close any gaps in the incident response plan of a ransomware attack.

Anthony: I agree with Colin. No amount of resources can keep a determined attacker out of your network. Community banks do have the benefit of having a smaller inventory of assets to manage, which reduces attack surfaces; however, the more banks allow employees to use personal devices for business, the more attack surfaces are introduced into the environment. Besides having an effective cyber awareness program, organizations should test and update their response plan. This includes periodically testing the movement of backup data into the production environment. Don't forget to back up and air-gap the network, hardware, and application configurations. They also should be periodically updated and tested.

Ahmed: Compared with larger banks, community banks are also more reliant on vendor-provided services to run critical functions. Management should consider the cyber hygiene[10] practices of MSSPs and TSPs, as they are certainly an attack vector. Community banks should also proactively review and audit access privileges given to the employees at MSSPs and TSPs and should even consider fourth-party risk management practices when reasonable.

[10] *Cyber hygiene* refers to the practices and steps taken to maintain the health and security of computer users, devices, networks, and data.

Has any new guidance been issued recently that community banks should know?

Ahmed: As far as guidance, earlier in 2022, the Federal Reserve and the federal banking agencies issued a joint final rule on computer-security incident notification requirements for banking organizations and their bank service providers.[11] This rule is intended to improve the sharing of information about cyber incidents to help promote early awareness of emerging threats and help agencies react to them. Be sure to read through Supervision and Regulation (SR) letter 22-4/Consumer Affairs (CA) letter 22-3 to familiarize yourself with the timing requirements for reporting a security incident to your regulator, as well as the appropriate communication channels.[12] SR letter 21-14 is another recent guidance issuance that reinforces the need for banks to effectively authenticate users and customers to protect information systems, accounts, and data.[13] If you've ever wondered about the regulatory view on multifactor authentication (MFA), this is a good place to start. The FFIEC also recently published an updated Architecture, Infrastructure, and Operations (AIO) booklet of its *Information Technology Examination Handbook*.[14] This new booklet replaces the previous Operations booklet, and, while it does not impose any requirements on banks, it's a good way for bank management to become familiar with prudent AIO functions.

Colin: While they're not new nor guidance for that matter, the Ransomware Self-Assessment Tool (RSAT) and the FFIEC Cybersecurity Assessment Tool (CAT) could be a good place for banks to start.[15,16] I would also suggest that a bank set up a process for receiving notifications from organizations such as the Cybersecurity and Infrastructure Security Agency (CISA) or the Financial Services Information Sharing and Analysis Center (FS-ISAC). These organizations can provide banks with information on new and emerging threats and implications for bank security programs. There are multiple organizations, such as the SysAdmin, Audit, Network, and Security (SANS) Institute, that send notifications pertaining to recent threats. Information captured within these missives might help a bank bolster its internal control environment.

Anthony: As Colin mentioned, CISA has many resources available to organizations to help them assess themselves and better prepare for a cyberattack. The New York Department of Financial Services (NYDFS) also recently provided ransomware guidance that lists a number of good practices that a bank can take to prevent and prepare for an incident.[17] Many other third parties also have resources, guidance, and tactics to help organizations better defend against and prepare for a cyberattack. Managers should select the proven tactic or practice that works best for their organization. What's important is that organizations need to *stay informed*. They need to track their data and system assets and identify their vulnerabilities, be aware of new cyber threats, and enforce good cyber hygiene practices. Threat actors are always looking for weaknesses in perimeter defenses and new tactics to deploy their attacks.

11 The joint final rule, "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers," is available at www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf.

12 SR letter 22-4/CA letter 22-3, "Contact Information in Relation to Computer-Security Incident Notification Requirements," is available at www.federalreserve.gov/supervisionreg/srletters/SR2204.htm.

13 SR letter 21-14, "Authentication and Access to Financial Institution Services and Systems" is available at www.federalreserve.gov/supervisionreg/srletters/sr2114.htm.

14 The AIO booklet of the *FFIEC Information Technology Examination Handbook* is available at https://ithandbook.ffiec.gov/media/402799/ffiec_itbooklet_aio.pdf.

15 Access the RSAT at www.csbs.org/ransomware-self-assessment-tool.

16 The CAT is available at www.ffiec.gov/cyberassessmenttool.htm.

17 The NYDFS industry letter on ransomware guidance is available at www.dfs.ny.gov/industry_guidance/industry_letters/il20210630_ransomware_guidance.

Do you have any words of warning or some common practices you may have seen that banks should avoid?

Colin: Years ago, I would hear management proclaim that they did not think the bad actors would come after them due to their size. Over the years we now see the flaw in that type of thought process. *Everyone is a target.* In fact, some bad actors specifically come after smaller institutions based on the belief that their internal controls will not be as robust as those of a larger institution. You have to assume that cyberattackers are knocking on your front door.

Anthony: Absolutely, banks are only as strong as their weakest link, and everyone is a target. There are plenty of improper practices management should avoid to better prepare. Among banks with weak security culture and awareness, I see:

- inadequate patching of vulnerabilities or mitigating risks from technology in a timely manner;
- inconsistent reviews of vulnerabilities and the risks posed to the bank; and
- a lack of resources dedicated to the development and implementation of a strong cyber awareness program.

Finally, you should never assume your cyber insurance will cover your losses. A bank should be aware of insurance policy provisions that require a bank to adopt certain cyber hygiene practices and to implement adequate controls. Controls such as MFA[18] may be required.

Ahmed: I'll also add that it's important to avoid taking a lax approach that allows employees to use their own devices to conduct bank business. The use of personal devices is common among community banks and introduces various risks to the organization, particularly when these practices are not properly managed. Ransomware can easily pass into a bank's network when an employee logs in to the network with a personal device that is carrying hidden ransomware code.

Therefore, I'd suggest management consider restricting personally owned devices on the bank network to reduce this risk. I also encounter many instances in which web access management is taken lightly or not properly configured. Weak management of employees' web access can allow ransomware to spread by employees unknowingly visiting an infected website. A proper web filtering program can provide protection against this type of ransomware risk, and I'd recommend that community bank IT teams use appropriate security products to block access to known ransomware sites.

Conclusion

Ransomware attacks are growing at an alarming pace. Ransomware attacks can jeopardize the safety and soundness of banks and can place extreme emotional stress on the employees of a compromised bank. However, the practices and approaches discussed in this article can help bank management prepare against an attack and regain some peace of mind. For more information on this topic and additional helpful guidance, reference the articles and online resources provided throughout this issue of *Community Banking Connections.* ■

[18] MFA requires the user to present two or more forms of evidence before being granted access. These include something the user knows (such as a password), something the user has (such as a physical token), and something the user is (such as a fingerprint).

Requirements for Notifying Primary Federal Regulators About Computer-Security Incidents

by Kalyn Yzaguirre, Senior Examiner/Supervisory Specialist, Examinations & Inspections, Federal Reserve Bank of Kansas City

Cyberattacks carried out against banks have been on the rise over the past several years. According to data from the Financial Crimes Enforcement Network (FinCEN), over 27,000 cyber-related suspicious activity reports were filed in 2021,[1] a 34 percent increase from the prior year. These attacks may take many forms, including ransomware, denial of service attacks, or account hijacking. In addition to targeting banks, malicious cyber actors may target third parties or those in the software supply chain.

Attackers are constantly altering their approaches to stay ahead of cyber defenders. As part of sound risk management, banks are expected to have plans in place to respond to cyber incidents. As discussed later in this article, the Federal Reserve and the other federal banking agencies require banking organizations to notify their primary federal regulator of a cyber incident (referred to as a computer-security incident) that has had, or will have, a material impact on the organization.

Final Rule Establishes Computer-Security Incident Notification Requirements

On November 23, 2021, the Federal Reserve Board, the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (collectively, the federal banking agencies) issued a notification rule that requires banking organizations[2] to notify their primary federal regulator of certain computer-security incidents.[3] In summary, the rule requires a banking organization to notify its primary federal regulator of a material computer-security incident (referred to as a notification incident) as soon as possible and no later than 36 hours after the banking organization determines that such an incident has occurred. As of May 1, 2022, banking organizations are expected to be in compliance with the notification rule.

The goal of this new regulation is to promote early awareness of emerging threats from computer-security incidents to banking organizations and the broader financial system. Not all computer-security incidents require notification. That said, the rule focuses on computer-security incidents that have had, or are likely to have, a material impact on a banking organization's operations or its ability to deliver banking products and services to a significant portion of its customer base.

The federal banking agencies expect that this new regulation will help promote early awareness of emerging threats to banking organizations and the broader financial system. Further, banks' prompt notification about an incident should help the agencies react to these threats before they become systemic.

Recognizing that many banks outsource critical operations and processes, the notification rule also applies to their service providers. Therefore, when there is a computer-security incident at a bank service provider, the service provider is required to notify its affected banking organization customers as soon as possible. The service provider provisions of the rule cover a computer-security incident that has caused or is likely to cause a material disruption or degradation in services for four or more hours.

What Is a Reportable Notification Incident?

After establishing that a computer-security incident has taken place, a bank must determine whether the incident qualifies as a notification incident under the rule. Two parts of the rule's definition of notification incident are most relevant to community banks. Specifically, a

[1] See FinCEN, "SAR Filings by Industry for the Period January 1, 2014, to December 31, 2021," available at www.fincen.gov/reports/sar-stats/sar-filings-industry. Trend data can be accessed by downloading the Excel file "Depository Institution" and selecting the tab marked "Exhibit 5."

[2] For purposes of the notification rule, ''banking organizations'' includes the following institutions supervised by the Federal Reserve: U.S. bank holding companies and savings and loan holding companies, state member banks, the U.S. operations of foreign banking organizations, and Edge and agreement corporations. The notification rule also applies to banking organizations supervised by the FDIC and the OCC.

[3] See 86 *Federal Register* 66,424 (November 23, 2021), available at www.govinfo.gov/content/pkg/FR-2021-11-23/pdf/2021-25510.pdf. See also 12 CFR 225.300–225.303.

Examples of Reportable Notification Incidents
1. A large-scale distributed denial of service attack disrupts customer account access for an extended period (e.g., more than four hours).
2. A bank service provider that is used by a banking organization for its core banking platform to operate business applications is experiencing widespread system outages and recovery time is undeterminable.
3. A failed system upgrade or change results in widespread user outages for customers and employees.
4. An unrecoverable system failure results in activation of the business continuity or disaster recovery plan.
5. A computer hacking incident disables the bank's operations for an extended period.
6. Malware on a bank's network poses an imminent threat to its core business lines or requires a bank to disengage any compromised products or information systems that support the bank's core business lines from internet-based network connections.
7. A ransom malware attack encrypts a core banking system or the bank's backup data.
Source: The preamble to the notification rule at www.govinfo.gov/content/pkg/FR-2021-11-23/pdf/2021-25510.pdf

notification incident is a computer-security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's:

1. ability to carry out banking operations, activities, or processes, or its ability to deliver banking goods and services to a material portion of its customer base in the ordinary course of business, or
2. business line(s), including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value to the bank.

See Examples of Reportable Notification Incidents for incidents that a bank should report. Ultimately, a bank must make its own determination regarding what is material to its financial condition and business operations.

Where and When to Report a Notification Incident

To comply with the rule, a Federal Reserve–supervised institution must report a notification incident to the Federal Reserve Board by email (incident@frb.gov) or by phone (866-364-0096). As previously mentioned, a supervised institution is expected to notify the Fed about a notification incident as soon as possible and no later than 36 hours after the bank determines a reportable incident has occurred.

The notification rule also requires a bank's service provider to notify its affected banking organization customers as soon as possible of a computer-security incident that is likely to cause a material disruption or degradation in services for four or more hours. Once a bank receives such a notice from its service provider, the bank must determine whether it is experiencing a notification incident. If this is the case, the bank is required to notify its primary federal regulator.

Information on Implementing the Notification Rule

Under the notification rule, there are no forms to complete. Further, a bank is not required to provide specific information in the notice to the primary federal regulator other than that a notification incident has occurred. Rather, the aim is to open a dialogue between the bank and its regulator. The Federal Reserve and the other federal banking agencies anticipate that a bank will need a reasonable amount of time to determine that it has experienced a notification incident. For example, if

Continued on page 19

Fintech Partnerships: What to Consider

by Ethan Jackson, Senior Technical Advisor, Strategy, Risk, and Innovation Team, Supervision, Regulation, and Credit, Federal Reserve Bank of Richmond, and Jessica Olayvar, Supervisory Analyst, Strategy, Risk, and Innovation Team, Supervision, Regulation, and Credit, Federal Reserve Bank of Richmond

Banks have historically engaged with technology firms to facilitate transactions and optimize internal processes. However, over the past several years, the variety of technology firms offering financial technology (fintech) services, new financial products, and digital enhancements to banks has rapidly increased. The article "A New Era of Banking: 12th District Community Banks Are Driving Innovation Through Fintech Partnerships," which appeared in the First Issue 2022 of *Community Banking Connections,* gave several examples of innovative partnerships pursued by community banks in the 12th District.[1] While there are countless reasons a bank may pursue a fintech partnership, understanding the partnership types and unique fintech due diligence considerations can help prospective bank partners effectively navigate this dynamic landscape.

Types of Fintech Partnerships

In early 2021, Federal Reserve staff held meetings with community bankers and other industry stakeholders across the country to better understand their risk management strategies and relationships with fintech firms. These conversations prompted the release of the paper "Community Bank Access to Innovation Through Partnerships," which categorized fintech engagements into three main types: (1) operational technology partnerships, (2) customer-oriented partnerships, and (3) front-end fintech partnerships.[2] The Figure highlights the differences between these three types of engagement given a bank's strategic needs.

These key considerations are relevant for all three types of partnerships:

- As a precursor to any type of partnership, establishing a robust third-party risk management program (see Due Diligence Considerations for Fintech Partnerships)
- Drawing on a cross-disciplinary team to identify key risks and plan for implementation
- Having relevant staff with the technical expertise to execute and maintain the third-party solution
- Developing contingency plans and considering the life cycle of the fintech partnership

Beyond these considerations, each type of partnership has its own specific benefits, risks, and challenges.

Operational Technology Partnership

In an operational technology partnership, a bank strives to gain efficiencies, streamline processes, enhance monitoring, and/or improve the ability to comply with regulatory requirements (sometimes called regulatory technology, or regtech). These behind-the-scenes partnerships aim to improve the bank's internal systems

[1] The article is available at https://cbcfrs.org/articles/2022/i1/vftd-new-era-of-banking-fintech.

[2] The September 2021 paper, which was released through Supervision and Regulation (SR) letter 21-16/Consumer Affairs (CA) letter 21-13, is available at www.federalreserve.gov/publications/files/community-bank-access-to-innovation-through-partnerships-202109.pdf. The SR/CA letter is available at www.federalreserve.gov/supervisionreg/srletters/SR2116.htm.

Figure: Types of Fintech Partnerships

Each partnership type between a community bank and a fintech targets specific needs and objectives of a community bank.

Source: "Community Bank Access to Innovation Through Partnerships," available at www.federalreserve.gov/publications/files/community-bank-access-to-innovation-through-partnerships-202109.pdf

and workflows, such as loan underwriting or fraud detection. One example of this could be a partnership that uses artificial intelligence (AI) to automate the credit decision or underwriting processes.

In this example, AI has the potential to expedite and streamline these processes. However, banks should align credit decisions with existing credit risk management policies and practices. Additionally, the use of AI in underwriting may increase the risk of introducing exclusionary bias toward protected classes, leading to fair lending concerns. This topic has gained prominence in recent years and is a key area of responsibility for the Consumer Financial Protection Bureau (CFPB).[3] Bank business lines, such as compliance and audit, should be involved in the due diligence and risk assessment process to mitigate the possibility of encountering issues later.

Customer-Oriented Partnership

Customer-oriented partnerships aim to enhance some aspect of a bank's underlying customer-facing platform without the fintech directly interacting with customers. Some examples of these partnerships are account opening tools or person-to-person money transfers. Community banks have traditionally been constrained to their geographical footprint. By enhancing the digital presence of community banks, customer-oriented partnerships could help community banks reach new customers[4] and satisfy existing customer demand. However, like any customer-facing product or service, this type of partnership, if not managed properly by a bank, can expose the bank to increased compliance or reputational risk.

For example, a bank exploring a fintech partnership that facilitates the opening of deposit accounts or loan originations should comply with its customer identification program, customer due diligence program, and beneficial ownership program to limit any Bank Secrecy Act (BSA) risks. Additionally, a bank failing to include appropriate disclosures on the newly enhanced customer-facing platform could be found to have Unfair or Deceptive Acts or Practices (UDAP).

Front-End Fintech Partnership

The least common but fastest-growing subset of partnerships is front-end facing, sometimes referred to as

[3] See Kate Berry, "CFPB Warnings of Bias in AI Could Spook Lenders," *American Banker*, January 31, 2022, available at www.americanbanker.com/creditunions/news/cfpb-warnings-of-bias-in-ai-could-spook-lenders.

[4] See Kate Rooney, "Small Banks You've Never Heard of Quietly Power the Booming Fintech Industry," CNBC, February 15, 2019, available at www.cnbc.com/2019/02/15/small-banks-youve-never-heard-of-quietly-power-the-booming-fintech-industry--.html.

Key Due Diligence Topics

1. Business Experience and Qualifications	2. Financial Condition	3. Legal and Regulatory Compliance
• Company overview • List of client references • Ownership information	• Financial statements and auditors' opinions • Annual reports • Market information on competitors	• Organizational documents and business licenses • Outstanding legal and regulatory issues
4. Risk Management and Controls	**5. Information Security**	**6. Operational Resilience**
• Policies, procedures, and other documentation • Self-assessments • Key risk indicator reports	• Information security controls assessments • Incident management and response policies • Incident reports	• Business continuity, disaster recovery, and incident response plans • Service-level agreements • Outsourcing policies

Source: *Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks*, available at www.federalreserve.gov/publications/files/conducting-due-diligence-on-financial-technology-firms-202108.pdf

banking-as-a-service or BaaS. In this type of partnership, a fintech firm interacts directly with a consumer by providing services or banking products using the bank's infrastructure. Under these agreements, the bank can be seen as a silent partner, and fintech customers often are not aware that a bank is involved in the service or transaction. By combining a fintech's technological capabilities with a bank's infrastructure, these partnerships often aim to grow deposits, diversify the bank's lending portfolio, and increase revenue streams.

Risks vary depending on the type of product offered through an established partnership and can include, but are not limited to, market, credit, liquidity, operational, third-party management, and compliance risk. For example, banks partnering with deposit-seeking fintech firms should prepare for a high volume of new customer acquisitions arising from the fintech firm and create contingency plans for unwinding the customer relationships and safeguarding liquidity if the fintech partnership is terminated. Additionally, newer fintech firms may be inexperienced when it comes to banking regulation, requiring enhanced compliance oversight and education.

Due Diligence Considerations for Fintech Partnerships

Banks are expected to conduct adequate due diligence prior to vendor selection for any outsourced partnership. SR letter 13-19/CA letter 13-21, "Guidance on Managing Outsourcing Risk," advises banks on the risks posed by service providers, the role of senior management, and, of course, due diligence considerations.[5] SR letter 13-19/CA letter 13-21 outlines three key aspects in a due diligence evaluation: (1) business background, reputation, and strategy; (2) financial performance and condition; and (3) operations and internal controls. This guidance is certainly relevant as bank senior management and board members consider prospective fintech partnerships.

In August 2021, the Federal Reserve Board, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency issued *Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks* as a resource geared toward this specific

[5] SR letter 13-19/CA letter 13-21 is available at www.federalreserve.gov/supervisionreg/srletters/sr1319.htm.

process.[6] While this guide builds on the expectations outlined in SR letter 13-19/CA letter 13-21, it describes the benefits and risks that arise in fintech partnerships and outlines six key topics for banks to consider during due diligence evaluations (see Key Due Diligence Topics). The guide further explains potential considerations and information sources that bankers could request from fintech companies to review during the evaluation period. For example, under the "Business Experience" section, the guide suggests reviewing the fintech's company overview, organizational charts, list of client references, volume and types of complaints, public records of legal and regulatory actions, media reports, and a summary of any past operational failures of the company. Bankers may use this guide as a supplement to their vendor risk management framework to evaluate potential fintech partnerships.

Conclusion

Banks seeking to establish new fintech partnerships are encouraged to begin their search with a clear idea of the bank's overall business goals and objectives. Similarly, it is important to have a thorough understanding of how a fintech firm's business strategy and risk profile align with the bank's established risk appetite and objectives. In general, a bank with a robust third-party risk management program that encourages cross-disciplinary input and considers the life cycle of a partnership is best positioned for an effective partnership.

Many community banks have attempted to stay abreast of evolving technologies by turning to various sources for guidance. For example, there has been a rise in community and regional bank–led incubators, consortiums, and associations focused on pooling resources for understanding, investing in, testing, and successfully implementing new technology. To improve their understanding of the dynamic fintech landscape, some bankers have had informal discussions with peer banks to learn from their experiences. Several state and federal regulators have launched staff units dedicated to facilitating communication and providing helpful information to fintech firms and bank partners. Banks are encouraged to reach out to Federal Reserve examination staff members for answers to questions about establishing and implementing fintech partnerships, including risk management expectations. ■

[6] See *Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks,* August 2021, available at www.federalreserve.gov/publications/files/conducting-due-diligence-on-financial-technology-firms-202108.pdf.

Continued from page 15

Requirements for Notifying Primary Federal Regulators About Computer-Security Incidents

an incident occurs outside of normal business hours, the Federal Reserve does not expect a supervised financial institution will be able to determine immediately that the incident is a notification incident under the rule. For additional guidance on implementation of the notification rule, Federal Reserve–supervised institutions should refer to the Fed's guidance, "Contact Information in Relation to Computer-Security Incident Notification Requirements," which includes information on how to contact the Federal Reserve.[4]

Summary

When it comes to cybersecurity, threat actors appear to be showing no signs of slowing down their attacks. The ultimate goal of the notification rule is to mitigate information security risks to U.S. banking organizations and safeguard our financial system. ■

[4] See Supervision and Regulation letter 22-4/Consumer Affairs letter 22-3, available at www.federalreserve.gov/supervisionreg/srletters/SR2204.htm. For nonmember state banks, refer to the FDIC Financial Institution Letter (FIL) 12-2022, and for national banks, refer to OCC Bulletin 2022-8.

2022 Writers' Cohort

Meet a Cohort Member

In this issue, Miles Green discusses the crash-course education he received when he became a Fed examiner during the Great Recession and the challenging conversations he had with senior bank leaders at the time. He also shares his overabundance of hobbies, talks about how his young daughter's interests are as varied as his, and reveals that if you want a refreshing cocktail on a summer day — you need to add the secret ingredient.

Miles Green

Advanced Examiner, Community and Regional Safety and Soundness, Supervision, Regulation, and Credit, FRB Richmond

How long have you been with the Fed?

I've been at the Federal Reserve Bank of Richmond for over 12 years. I started as a safety and soundness examiner in 2009 while the Great Recession was still inflicting its turmoil on the banking industry. After only a few months of learning the ropes in the office, I joined examination teams in the field. The role was fast-paced and challenging. I remember being nervous when talking through tough topics with bank senior leaders while onsite at their institutions. The bankers showed understanding with my inexperience at the time, and that treatment was foundational to my current philosophy of conducting supervision built on strong relationships. I spent 40 weeks on the road in 2010, traveling from bank to bank across the Fifth District. That period was a true crash-course education for me. It was difficult at times, but I am thankful today for the many lessons I learned early on in my career.

What hobbies or activities are you most passionate about?

My friends poke fun at me by saying that my hobby is collecting hobbies. I'm like a bird attracted to shiny objects. I love trying new things. A tailored-down list of interests from just the last few years includes long-distance running, CrossFit, rock climbing, tennis, table tennis, pickleball, cooking, board games, mixing cocktails, building a vinyl collection, and trading stocks. I was a year ahead of the sourdough bread baking pandemic trend. My neighborhood in Richmond, VA, hosts a world-class bakery, and I was lucky to obtain a sample of their sourdough starter a few years back. Now each holiday season, I bake sourdough loaves for friends and family. In August 2020, my wife and I had our first child, Georgie Green. My hobbies are on pause for a stretch as most of my energy goes into parenting. My daughter has a variety of interests just like her dad. She loves riding in *beep-beeps* and *choo-choos*, reading books about *meow-meows* and *woof-woofs*, and practicing her backstroke at the pool.

If you could visit any place in the world for a month, where would you go and why?

For shorter trips, my travel motivations usually include family time, relaxation, entertainment, or the draw of good food. The longest vacations of my life have never extended beyond a couple weeks. If I had the freedom to escape for a month to any destination, I would pick Colorado. There are a handful of activities that I wish I had learned as a kid because I now find them unapproachable as an adult. Skiing is at the top of that list. I'm told that it takes the average person one to three weeks to learn how to ski. I would love to visit Colorado for a month and dedicate myself to picking up this activity that I've always imagined I would enjoy.

If for six months you didn't have to worry about money or personal or professional obligations, how would you spend that time?

I've had a period of my life where I had an opportunity like this. After graduating from college in 2009, I took six months for myself to live worry free before "real life" started. I mostly spent the days fishing. This pursuit started because my father gave me a baitcasting fishing reel as a graduation gift. He is an avid fisherman and wanted to share his favorite activity with me. My initial excursion to test out my new gift ended in disaster. I botched my first cast, which bird-nested the entire spool of line, and I ended up going home after five minutes. Frustration from that moment turned into determination to get better, which then turned into an obsession with fishing. Every day of that summer, I was either on a lake or a river in my kayak. The hobby even evolved into competition fishing for a period. I participated in bass fishing tournaments across Virginia and North Carolina up until I started working full time at the Fed.

Have you ever completed anything on your bucket list? If so, what was it?

I'm a huge tennis fan. I record and watch every match of major tennis tournaments. One of my bucket list items was to watch a tennis major from the spectator stands instead of my living room couch. I checked this wish off my list when I attended the 2019 U.S. Open in Flushing Meadows, NY. My wife and I saw many of our favorite players, including Serena Williams, Roger Federer, Rafael Nadal, and Novak Djokovic. It's true that Rafa practices as hard as he plays. They rotated three different training partners in and out during his warm-up session because of how much he ran them around. We were fortunate to attend a breakout match of American tennis rising star Coco Gauff. We were also there for Daniel Medvedev's epic meltdown that other tennis fans will remember. Even with witnessing all the amazing play, my wife and I agree a main highlight of the experience was walking the grounds and enjoying the atmosphere while sipping the U.S. Open's signature cocktail, the "Honey Deuce." Do yourself a favor and try this refreshing drink on a hot summer day. Recipe: Grey Goose vodka, lemonade, black raspberry liqueur, and frozen honeydew melon balls (key ingredient).

Cohort Chair:

Kerri Allen, Examiner, Examinations & Inspections, FRB Kansas City

Cohort Advisor:

J.M. Nemish, Senior Examiner, Supervision, Regulation, and Credit, FRB Richmond

Cohort Members:

Stacy Barilla, Examiner, IT Examinations – CBO & Service Providers, Supervision, Regulation, and Credit, FRB Philadelphia, **Ray Bolton**, CRSB Examiner, Supervision and Regulation, Regional and Community Supervision, FRB Chicago, **Miles Green**, Advanced Examiner, Community and Regional Safety and Soundness, Supervision, Regulation, and Credit, FRB Richmond, **William Mark,** Lead Examiner, Supervision and Regulation, FRB Chicago, **Jessica Olayvar,** Supervisory Analyst, Strategy, Risk, and Innovation Team, Supervision, Regulation, and Credit, FRB Richmond, **Carla Thomas,** Examiner, Regional, Community and Foreign Supervision, Supervision + Credit, FRB San Francisco, **Kalyn Yzaguirre,** Senior Examiner/ Supervisory Specialist, Examinations & Inspections, FRB Kansas City

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 all the Federal Reserve Board's rulemakings, press releases, testimonies, speeches, and policy statements, visit the Federal Reserve's website at www.federalreserve.gov/.

ACTIONS

Actions Related to Safety and Soundness Policy

On September 8, 2022, the Federal Reserve Board issued a policy statement promoting the submission of whistleblower claims regarding misconduct, unsafe or unsound practices, or violations of law or regulation for Fed-supervised banking organizations. Supervision and Regulation (SR) letter 22-7 and Consumer Affairs (CA) letter 22-7 are available at www.federalreserve.gov/supervisionreg/srletters/SR2207.htm.

On August 16, 2022, the Federal Reserve Board provided additional information for banking organizations engaging or seeking to engage in crypto-asset–related activities. SR letter 22-6 and CA letter 22-6 are available at www.federalreserve.gov/supervisionreg/srletters/SR2206.htm.

On July 6, 2022, the federal banking agencies issued a joint statement to remind banks of the risk-based approach to assessing customer relationships and conducting customer due diligence. SR letter 22-5 is available at www.federalreserve.gov/supervisionreg/srletters/SR2205.htm.

Actions Related to Consumer Policy

On May 5, 2022, the Task Force on Consumer Compliance of the Federal Financial Institutions Examination Council released a revised version of "A Guide to HMDA Reporting: Getting It Right!" The updated guide is intended to assist financial institutions in complying with the Home Mortgage Disclosure Act (HMDA) as implemented by the Consumer Financial Protection Bureau's Regulation C. CA letter 22-4 is available at www.federalreserve.gov/supervisionreg/caletters/caltr2204.htm.

Other Board Actions and Releases

The Federal Reserve announced the pending release of a second tool to help community financial institutions implement the Current Expected Credit Losses, or CECL, accounting standard. Known as the Expected Losses Estimator, or ELE, the spreadsheet-based tool uses a financial institution's loan-level data and management assumptions to aid community financial institutions in calculating their CECL allowances. The June 7, 2022, press release is available at www.federalreserve.gov/newsevents/pressreleases/bcreg20220607a.htm.

Five federal regulatory agencies jointly issued revised questions and answers regarding federal flood insurance law and the agencies' implementing regulations. The May 11, 2022, press release is available at www.federalreserve.gov/newsevents/pressreleases/bcreg20220511a.htm.

Federal bank regulatory agencies jointly issued a proposal to strengthen and modernize regulations implementing the Community Reinvestment Act (CRA) to better achieve the purposes of the law. The May 5, 2022, press release is available at www.federalreserve.gov/newsevents/pressreleases/bcreg20220505a.htm.

SPEECHES

Speeches Related to Supervision and Regulation

Vice Chair of Supervision Michael S. Barr gave a speech at the Brookings Institution, Washington D.C., on September 7, 2022. His speech, titled "Making the Financial System Safer and Fairer," is available at www.federalreserve.gov/newsevents/speech/barr20220907a.htm.

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

Governor Christopher J. Waller gave a speech at the Rocky Mountain Economic Summit Global Interdependence

Center, Victor, ID, on July 14, 2022. His speech, titled "Monetary Policy in a World of Conflicting Data," is available at www.federalreserve.gov/newsevents/speech/waller20220714a.htm.

Vice Chair Lael Brainard gave a speech at the Bank of England Conference, London, on July 8, 2022. Her speech, titled "Crypto-Assets and Decentralized Finance Through a Financial Stability Lens," is available at www.federalreserve.gov/newsevents/speech/brainard20220708a.htm.

Governor Michelle W. Bowman gave a speech at the Executive Officers Conference, Massachusetts Bankers Association, Harwich, MA, on June 23, 2022. Her speech, titled "The Outlook for Inflation and Monetary Policy," is available at www.federalreserve.gov/newsevents/speech/bowman20220623a.htm.

Governor Christopher J. Waller gave a speech at the "Monetary Policy at a Crossroads" panel discussion hosted by the Dallas Society for Computational Economics, Dallas, on June 18, 2022. His speech, titled "Lessons Learned on Normalizing Monetary Policy," is available at www.federalreserve.gov/newsevents/speech/waller20220618a.htm.

Chair Jerome H. Powell gave welcoming remarks at the "International Roles of the U.S. Dollar" research conference sponsored by the Federal Reserve Board, Washington, D.C., on June 17, 2022. His remarks are available at www.federalreserve.gov/newsevents/speech/powell20220617a.htm.

Governor Christopher J. Waller gave a speech at the SNB-CIF Conference on Crypto Assets and Financial Innovation, Zürich, Switzerland, on June 3, 2022. His speech, titled "Risk in the Crypto Markets," is available at www.federalreserve.gov/newsevents/speech/waller20220603a.htm.

Governor Christopher J. Waller gave a speech at the Institute for Monetary and Financial Stability Distinguished Lecture, Goethe University, Frankfurt, Germany, on May 30, 2022. His speech, titled "Responding to High Inflation, with Some Thoughts on a Soft Landing," is available at www.federalreserve.gov/newsevents/speech/waller20220530a.htm.

Chair Jerome H. Powell gave welcoming remarks at the Reservation Economic Summit 2022 hosted by the National Center for American Indian Enterprise Development, Las Vegas, (via prerecorded video) on May 24, 2022. His remarks are available at www.federalreserve.gov/newsevents/speech/powell20220524a.htm.

Governor Christopher J. Waller gave a speech at the 2022 Hoover Institution Monetary Conference, Stanford, CA, on May 6, 2022. His speech, titled "Reflections on Monetary Policy in 2021," is available at www.federalreserve.gov/newsevents/speech/waller20220506a.htm.

Other Speeches

Vice Chair Lael Brainard gave a speech at the National Native Coalition Virtual Series on the Community Reinvestment Act Notice of Proposed Rulemaking (via webcast) on July 19, 2022. Her speech, titled "Strengthening the CRA: A Conversation with Representatives of Native Communities," is available at www.federalreserve.gov/newsevents/speech/brainard20220719a.htm.

Vice Chair Lael Brainard gave commencement remarks at the 2022 Commencement of the School for Advanced International Studies, Johns Hopkins University, Washington, D.C., on May 25, 2022. Her remarks are available at www.federalreserve.gov/newsevents/speech/brainard20220525a.htm.

TESTIMONIES

Vice Chair Lael Brainard testified on Digital Assets and the Future of Finance: Examining the Benefits and Risks of a U.S. Central Bank Digital Currency Report before the Committee on Financial Services, U.S. House of Representatives, Washington, D.C., on May 26, 2022. The testimony is available at www.federalreserve.gov/newsevents/testimony/brainard20220526a.htm.

Chair Jerome H. Powell testified on the Semiannual Monetary Policy Report before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, Washington, D.C., on June 22, 2022. Chair Powell submitted identical remarks to the Committee on Financial Services, U.S. House of Representatives, on June 23, 2022. The testimony is available at www.federalreserve.gov/newsevents/testimony/powell20220622a.htm.


FEDERAL RESERVE SYSTEM

SPECIAL ISSUE CYBERSECURITY

COMMUNITY BANKING CONNECTIONS

A SUPERVISION AND REGULATION PUBLICATION

Technology and Innovation in Community Banking: Opportunities, Challenges, and the Fed

Third Issue 2022

by Raphael W. Bostic, President and Chief Executive Officer, Federal Reserve Bank of Atlanta

Raphael W. Bostic

Community banks are beset by challenges on numerous fronts. Foremost among them is the relentless advance of technology and, along with it, heightened customer expectations for convenience and instantaneous service.

At a time when consumers and business customers can readily turn to digital offerings for all manner of financial services, traditional financial institutions must keep pace to remain relevant. This can be particularly tough for community banks, which typically face resource constraints — human, financial, and otherwise. As a result, meeting customer demands for technology-enabled services often means seeking help from partners. Partnerships with third-party firms can entail supplying services such as mobile banking directly to customers or, in some cases, offering services inside a physical branch.

Often these service providers are financial technology companies, or fintechs. These sorts of companies normally have roots in the information technology industry and thus may not instinctively understand the regulatory and fiduciary obligations that are second nature to banks.

In this space, I would like to share a few thoughts on the Federal Reserve's role in helping community banks address both the opportunities and the challenges that technology and innovation present. In particular, I will discuss third-party partnerships because they are especially important for community banks in today's financial services marketplace.

Facilitating Community Bank Engagement with Innovation

What role can the Fed play as community banks seek to navigate this new and challenging competitive landscape? Most important, in our capacity as a safety-and-soundness supervisor, we are committed to helping community banks pursue technology innovation, and thus engage with service providers, in a safe, sound, and responsible manner.

In my view, this work dovetails perfectly with our Reserve Bank's strategic priority to build an economy that works

Connect with Us

With each issue of *Community Banking Connections*, we aim to highlight the supervisory and regulatory matters that affect you and your banking institution the most, providing examples from the field, explanations of supervisory policies and guidance, and more. We encourage you to contact us with any ideas for articles so that we can continue to provide you with topical and valuable information.

Direct any comments and suggestions to editor@communitybankingconnections.org.

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