SECTION 5
Operational and Cyber Risks

- **Operational risks remain critical to banks as malicious cybercrime activities evolve and become more sophisticated.**
- **Ransomware and supply chain attacks continue to threaten banks and their third parties and remain an important source of risk to the financial industry.**
- **Geopolitical events continued to increase the likelihood of cyber-attacks on banks in 2023.**
- **While the use of checks has declined, check fraud continued to rise.**
- **Adoption of quantum computing and generative artificial intelligence can pose new risks to critical infrastructure systems.**

Operational risks remain critical to banks as malicious cybercrime activities evolve and become more sophisticated, and as banks adopt new technologies. According to the 2023 Annual Survey of Community Banks conducted by the Conference of State Bank Supervisors and state financial regulators, cybersecurity continues to be a top internal risk priority for community banks. Nearly 92 percent of respondents cited cybersecurity as an either "extremely important" or "very important" risk priority.[62] Technology advances require bank managers to continuously improve cybersecurity and other internal controls to create operational resilience and mitigate the risk that their bank will suffer a significant service disruption.

Ransomware actors continue to target banks and their third parties. The term "ransomware" initially was used to describe malicious software designed to encrypt files on a device until a ransom was paid for the decryption method. However, in 2023 ransomware actors shifted from data encryption to data exfiltration techniques, demanding that victims pay a ransom to keep them from exposing stolen data. In either scenario, ransomware can disrupt core business activities, result in operational outages, threaten the confidentiality of customer data, and lead to a loss of confidence. Banks reduce the risk of a ransomware attack's success and minimize its negative impacts by applying effective cybersecurity risk management and mitigation principles, including the use of multifactor authentication, hardening of systems configurations, and timely patch management.

Ransomware threat actors continue to leverage known software vulnerabilities, phishing emails, texts targeting employees, and compromised credentials to gain access to networks through remote access. The 2023 Verizon Data Breach Investigation Report stated that 74 percent of breaches involved the human element, which includes social engineering attacks, errors, or misuse.[63] According to the IBM Cyber Security Intelligence Index for 2023, phishing was the preferred method (identified in 41 percent of incidents) that malicious cyber actors used to gain access to victimized networks and devices.[64] To heighten the likelihood of a compromise, phishing attacks used spear phishing tactics to deceive victims into clicking on unsafe links or opening infected attachments.

The Ransomware-as-a-Service (RaaS) model remains a key driver for the ongoing frequency of ransomware attacks. In this model, expert cyber actors assist less-experienced actors to become proficient at ransomware attacks. With plentiful access to RaaS kits and related support, criminals lacking the skill to develop their own malware can launch ransomware attacks quickly and affordably. In 2023, the average amount of "breakout time" for cybercriminals—or how long it took to go from initial access of a victimized network to accessing other previously untouched segments of that network (and possibly another

[62] Conference of State Bank Supervisors, "2023 CSBS Annual Survey of Community Banks," October 4, 2023.

[63] Verizon, "2023 Data Breach Investigation Report," June 6, 2023.

[64] IBM, "Cyber Security Intelligence Index for 2023," February 22, 2023.

partner-enterprise's connected network)—was 79 minutes, a five-minute drop from 2022. Breakout time for cybercriminals has been as fast as seven minutes.[65]

Supply chain attacks on third-party providers of software, hardware, and computing services remain an important source of risk to the financial industry. Compromised third-party software can result in disclosure of credentials or confidential data, corruption of data, installation of malware, and application outages. For example, in May 2023, the ransomware group Cl0p began exploiting a since-patched vulnerability in a widely used file transfer software called MOVEIt. The MOVEIt campaign targeted the U.S. financial sector and other enterprises globally. By July 2023, Cl0p was responsible for more than 170 attacks.

Geopolitical events continued to increase the likelihood of cyber-attacks on banks in 2023. Events like the Israel-Hamas conflict and the war in Ukraine have led to increased cyber-attacks targeting critical infrastructure around the world. In 2023, there was an observed increase in politically motivated, distributed denial of service (DDoS) attacks against financial sector participants and others. The Microsoft Digital Defense Report, published in October 2023, stated that while U.S. entities continued to be primary targets for DDoS attacks (54 percent of all attacks), Europe climbed to the second highest with 14 percent of attacks, overtaking East Asia. The change is tied to geopolitical conflicts, with pro-Russian "hacktivist" (cyber hackers with activist sensibilities) groups intensifying their attacks against Europe and the United States.[66] Hacktivist cyber-attacks observed related to the Israel-Hamas conflict include targeting of Israeli-manufactured information technology components and software, regardless of where they are deployed.

While the use of checks has declined, check fraud continued to rise. Fraudsters are stealing mail from U.S. Postal Service boxes and sorting through envelopes to look for checks being used to pay bills. Once obtained, bad actors are using chemical and electronic means to alter the amounts and payees on the checks and then depositing them using mules. Fraudulently altered checks can cause significant losses to financial institutions and disrupt bank operations.

Because of a nationwide surge in check fraud schemes targeting the U.S. mail, the Financial Crimes Enforcement Network (FinCEN) issued an alert to financial institutions to be vigilant in identifying and reporting such activity.[67]

Quantum computing will pose new risks to critical infrastructure systems. Quantum computing promises greater computing speed and power; however, it also has the potential to weaken or incapacitate current encryption methods. Traditional encryption generally relies on complex mathematical problems (encryption algorithms) that take an immense amount of time for classic computers to solve without knowing the encryption key. However, quantum computers use a different computing architecture that can solve certain types of problems much faster, including some encryption algorithms. Quantum computing is expected to eventually render public, current encryption methods useless. The Cybersecurity and Infrastructure Security Agency, the National Security Agency, and the National Institute of Standards and Technology issued a joint factsheet to encourage the early planning for migration to postquantum cryptographic standards by developing a Quantum-Readiness Roadmap.[68]

Generative Artificial intelligence (AI) technologies are being leveraged to circumvent identity- and authentication-based financial institution network defenses and perpetrate other frauds. Financial crime perpetrators are increasingly using AI to create fake or altered documentation, audio files, and video recordings, leading to increasing fraud cases.[69] The pervasiveness of generative AI tools allow malicious actors to easily leverage the technology to create more convincing or realistic content or materials to further fraud schemes.[70] Generative AI, including large language models, can augment live videos via "deepfakes" or voice cloning tools, making it more difficult for financial institutions to discern real versus fake identities during verification processes.

[65] CrowdStrike, "2023 Threat Hunting Report," August 8, 2023.

[66] Microsoft, "Microsoft Digital Defense Report 2023," October 2023.

[67] FinCEN, "FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail," FIN-2023-Alert003, February 27, 2023.

[68] Cybersecurity and Infrastructure Security Agency, "Quantum-Readiness: Migration to Post-Quantum Cryptography," August 21, 2023.

[69] Sift, "Q2 2023 Digital Trust & Safety Index – Fighting Fraud in the Age of AI and Automation," June 22, 2023.

[70] Precedence Research, "Generative AI Market Growth Is Booming With 27.02%," July 11, 2023.