Congressional Research Service
Informing the legislative debate since 1914

# Banking, Data Privacy, and Cybersecurity Regulation

Updated March 13, 2023

**Congressional Research Service**
https://crsreports.congress.gov
R47434

**CRS REPORT**
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R47434

March 13, 2023

**Andrew P. Scott**
Analyst in Financial Economics

**Paul Tierno**
Analyst in Financial Economics

# Banking, Data Privacy, and Cybersecurity Regulation

Financial data contains significant amounts of sensitive information, and ensuring the privacy of such data among financial institutions is a goal of many policymakers. In particular, Congress has demonstrated an interest in prioritizing data privacy standards in the financial system. Much of the legislative and regulatory data privacy framework established for banks and credit unions is constructed from a patchwork of cybersecurity provisions. Similarly, the implementation of cybersecurity supervisory programs among financial institution regulators is fragmented, and potential risks to the financial system have emerged as new technologies evolve.

Cybersecurity threats pose *operational risk*, *reputational risk*, and, potentially, *systemic risk*. Operational risk is the threat that an event such as a natural disaster, pandemic, or cyberattack limits or completely obstructs an institution's ability to do business. Reputational risk is the threat that customers will avoid future business with an institution due to such an event. Systemic risk is the threat that an event may trigger instability in an entire industry or the overall economy.

No single law provides a framework for regulating cybersecurity in the United States. Instead, several laws cover different industries, and numerous laws cover aspects of cybersecurity for the financial system. The Gramm-Leach-Bliley Act of 1999 (GLBA; P.L. 106-102) is the most comprehensive of these laws and directs financial regulators to implement disclosure requirements and security measures to safeguard private information. GLBA provides a cybersecurity framework built upon two pillars: (1) privacy standards that impose disclosure limitations or limit financial institutions concerning disclosure of consumers' information, and (2) security standards that require institutions to implement certain practices to safeguard the information from unauthorized access, use, and disclosure. The two major rules for implementing this framework are known as the Privacy Rule (Regulation P) and the Safeguards Rule, respectively. Other laws—such as the Sarbanes-Oxley Act of 2002 (P.L. 107-204), Fair and Accurate Credit Transactions Act (FACT Act; P.L. 108-159), Bank Protection Act (P.L. 90-389), and Bank Service Company Act of 1962 (P.L. 87-856)—complete the general legislative framework for depository institution cybersecurity.

Banking regulators implement the cybersecurity legislative framework through rulemaking, and then supervise institutions to ensure that banks are following regulations. Oversight of bank cybersecurity reflects a complex and sometimes overlapping array of state and federal laws, regulators, regulations, and guidance—many of which predate the emergence of cybersecurity risk. Congress is debating the extent to which it should unify or modernize the legislative framework for depository institutions. For example, one issue is how new technologies that facilitate financial data sharing should be treated under the existing cybersecurity framework. Another issue is how and whether the data privacy protections that exist for data sharing should also apply to data collection. The Data Privacy Act of 2023 (H.R. 1165), which the House Financial Services Committee ordered to be reported as amended in February 2023, examines several of these issues. Further, technology partnerships, particularly at smaller banks, with institutions such as cloud management companies, has led to new cybersecurity risks to the banking system. This has raised concerns among policymakers about the capacity of the existing framework to address new risks.

# Contents

Introduction ..... 1
Cybersecurity Risks to the Banking System ..... 1
Current Legislative Framework ..... 2
Recent Legislative Developments ..... 3
Regulatory Framework ..... 4
GLBA Data Privacy and Safeguards ..... 4
GLBA Rulemaking Authorities ..... 5
Recent Updates on Depository Regulation of GLBA Cybersecurity Provisions ..... 5
Other Regulatory Developments ..... 6
Supervisory Process ..... 7
GLBA Supervision ..... 7
Depository Institution Supervision ..... 7
Third-Party Service Providers ..... 8
Policy Issues for Congress ..... 9
Data Privacy ..... 10
Technology Service Providers ..... 10
Cloud Computing ..... 10

## Tables

Table 1. Regulatory Jurisdiction for Different Banking Institutions ..... 4
Table 2. Summary of Privacy and Safeguards Rules ..... 5
Table 3. Relevant Rulemaking Authority for GLBA ..... 5
Table 4. Supervision and Enforcement Authority for GLBA ..... 7
Table 5. Depository Supervision Toolkit for Cybersecurity ..... 8

## Contacts

Author Information ..... 11

# Introduction

Cybersecurity is a major concern of banks and banking regulators. Data breaches at large financial institutions and credit reporting agencies have increased concern about the privacy and security of the large amounts of consumer financial information that these companies gather, use, and store.[1] Many in Congress have demonstrated an interest in data privacy and cybersecurity, as evidenced by a number of hearings on large-scale data breaches in prior Congresses. In the 118th Congress, the Chair of the House Financial Services Committee identified data privacy as a legislative priority for the current session.[2] This report examines the existing legislative framework for financial cybersecurity, and provides some context for how regulators currently promulgate, supervise, and enforce various data privacy provisions.

The implementation of cybersecurity policy among banking regulators is fragmented, and potential risks to the financial system have emerged as new technologies evolve. This report focuses on the cybersecurity regulatory framework among the federal banking regulators—the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Federal Reserve—as well as the National Credit Union Administration (NCUA) and the Consumer Financial Protection Bureau (CFPB).

# Cybersecurity Risks to the Banking System

Cybersecurity means protecting systems, networks, devices, and data from digital attacks by criminals and other adversaries.[3] Cybersecurity threats pose *operational risk*, *reputational risk*, and, potentially, *systemic risk*.[4]

**Operational risk** is the threat that an event such as a natural disaster, pandemic, or cyberattack limits or completely obstructs an institution's ability to do business. Banks face risk from cyber threats, which could interrupt their daily operations.

**Reputational risk** is the threat that customers will avoid future business with an institution due to an event such as a cyberattack. The financial system depends on trust. For example, if a breach at a bank results in the release of personal data, customers may be reluctant to continue their relationship with the bank. They may choose to pull their deposits out from the bank and close

[1] For example, in spring and summer 2017, Equifax, one of the big three credit reporting agencies, announced that hackers had gained unauthorized access to the company's data, including that of 145 million customers. The data included Social Security numbers and drivers licenses. According to media reports, hackers were able to access the company's computer systems and consumer data for around two months before they realized it. See, for example, Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth, et al., " Equifax Says Cyberattack May Have Affected 143 Million in the U.S.," *The New York Times*, September 7, 2017, at https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html. For an overview of cyber incidents involving financial firms dating back to 2007, see *Timeline of Cyber Incidents Involving Financial Institutions*, Carnegie Endowment for International Peace, at https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#click-hide.

[2] For example, on February 23, 2023, the House Committee on Financial Services scheduled a markup of several bills in February 2023, including the "Data Privacy Act of 2023." For more, see https://financialservices.house.gov/uploadedfiles/hmkp-118-ba00-20230228-sd002-u1.pdf.

[3] See "Cybersecurity Awareness," Federal Financial Institution Examination Council, at https://www.ffiec.gov/cybersecurity.htm.

[4] For more on this landscape, see CRS Insight IN11621, *Cross-Cutting Issues in Cybersecurity: Financial Institutions*, by Chris Jaikaran and Andrew P. Scott; and CRS In Focus IF11717, *Introduction to Financial Services: Financial Cybersecurity*, by Andrew P. Scott and Paul Tierno.

their accounts. Without trust that customers' money and personal data are safe, the financial system cannot operate smoothly.

**Systemic risk** is the threat that a cyberattack may affect more than just the institution targeted and may jeopardize an industry or the entire economy. Banks, particularly large ones, can be highly interconnected, and many institutions depend on the same technological infrastructure. Thus, an attack on one information technology (IT) system could result in significant losses across the entire industry, both by costing the bank money to repair damages, and also the correlated risks that stem from consumers avoiding future business with the bank or other banks with similar exposure. Financial regulators consider the systemic risks to the entire industry. In doing so, they seek to ensure the safety and soundness not only of individual organizations but also their partners. The Financial Stability Oversight Council (FSOC) has identified three channels through which a cybersecurity event could threaten the stability of the U.S. financial system:[5]

1. Disrupting a key financial service or a financial market utility for which there are few substitutes (e.g., the central bank, securities and derivatives exchanges, and payment clearing and settlement institutions);
2. Causing a loss of confidence among a broad set of customers or market participants; and
3. Compromising the integrity of critical data (e.g., altering balance sheets), rendering information critical to financial firms either inaccurate or unusable.

Systemic risk from cybersecurity may have increased in 2020, as the pandemic has increased reliance on technology (e.g., remote payment systems, among others).

# Current Legislative Framework

No single law provides a framework for regulating cybersecurity in the United States. Instead, multiple laws cover different industries or cover aspects of cybersecurity for the broader financial system, while others apply more directly to banks. Some of these laws require financial regulators to establish cybersecurity standards for financial institutions, and provide regulators the authority to ensure compliance with such standards. Other laws provide broad authority to regulators to supervise some financial institutions for safety and soundness.

The **Gramm-Leach-Bliley Act of 1999** (GLBA; P.L. 106-102) is the most comprehensive of these laws and directs financial regulators to implement disclosure requirements and mandate security measures to safeguard private information. Specifically, Subtitle A of Title V of GLBA provides a framework for regulating data privacy and security practices for financial institutions.

The **Sarbanes-Oxley Act of 2002** (P.L. 107-204) requires certain corporations, including banks, to identify internal and external risks to their business and the ways that the company guards against those risks.

The **Fair and Accurate Credit Transactions Act of 2004** (FACT Act; P.L. 108-159) amended the Fair Credit Reporting Act to require regulatory agencies to develop identity theft guidelines, which outline "patterns, practices, and specific forms of activity that indicate the possible existence of identity theft" (15 U.S.C. §1681).

There are also two relevant laws specific to banks.

[5] FSOC, Annual Report 2022, p. 66, at https://home.treasury.gov/system/files/261/FSOC2022AnnualReport.pdf.

The **Bank Protection Act** (1968) (P.L. 90-389), as amended in 2010, directs the federal bank regulators to establish minimum security standards for banks and savings associations to "discourage robberies, burglaries, and larcenies" (12 U.S.C. §§1881-1884). Although the law does not mention cybersecurity specifically, the statutory language is broad enough to include protection against cyber threats.[6]

Other federal laws, such as the **Bank Service Company Act of 1962** (BSCA; P.L. 87-856) and the laws that establish the authorities for financial regulators to conduct safety and soundness examinations, allow regulators to supervise financial institution activities and partnerships (e.g., with technology service providers). Regulators rely on these broad authorities to shape and impose cybersecurity regulations on the institutions they regulate. For example, the banking regulators conduct on-site examinations under their authority to examine banks for safety and soundness and can require banks to take remedial action if their cybersecurity policies are deficient.

## Recent Legislative Developments[7]

Division Y of the Consolidated Appropriations Act, 2022 (P.L. 117-103) requires that "covered entities" report a "covered cyber incident" to the Cybersecurity and Infrastructure Security Agency within 72 hours and a ransomware payment within 24 hours of occurrence, respectively.[8] Covered incidents include, at a minimum, any incident that leads "to substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes."

On February 8, the House Financial Services Committee held a hearing[9] on various efforts to update bank regulation, including a discussion draft on data privacy. On February 28, 2023, the committee held a markup of several bills, including the Data Privacy Act of 2023 (H.R. 1165), introduced by Chair McHenry.[10] The bill would amend GLBA, clarify the inclusion of data aggregators[11] under the scope of the law, and give consumers some added control over certain data, such as the ability to access and remove it from financial institution records. Also, the draft includes a national preemption measure, which would supersede state law.[12] During the markup, a number of amendments were introduced. While all eight amendments introduced by Democrats

[6] For example, 12 C.F.R. §208.61 states that a bank must develop and maintain a security program and devices that ensure protection against robberies and other crimes.

[7] There are a number of legislative developments (e.g., H.R. 3912 and H.R. 3911) that pertain more broadly to cybersecurity policy and could impact the banking sector. The scope of this paper is limited to data privacy among banking regulators and depository institutions, and the legislation noted in this section reflects only bills that became law or bills in the current Congress that are being acted upon, which directly impact those entities.

[8] The term "covered entity" applies to "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21." The financial sector is included in the Policy Directive as a critical infrastructure sector. For more, see https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[9] U.S. House Financial Services Committee, "Hearing Entitled: Revamping and Revitalizing Banking in the 21st Century, February 8, 2023, at https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=408512.

[10] In this report, references to this bill are made to the amendment in the nature of a substitute, which can be found at https://docs.house.gov/meetings/BA/BA00/20230228/115381/BILLS-118-HR1165-M001156-Amdt-12.pdf.

[11] Data aggregators are entities that pull together various data to analyze and yield additional insights. This could be information that is public, such as names, geographical locations, and time, or more sensitive data such as account numbers.

[12] U.S. Congress, House Committee on Financial Services, *To Amend the Gramm-Leach-Bliley Act to [Modernize the Protection of the Nonpublic Personal Information of Consumers*, discussion draft.

were rejected, the committee adopted a substitute amendment that would "allow exceptions for disclosures of personal information permitted under the Gramm-Leach-Bliley Act. The amendment also would specify that disclosure of data retention policies would include the period of time data is held and the criteria the institution uses to determine that time."[13] The bill was ordered to be reported to the full House, as amended, by a vote of 26-21.

# Regulatory Framework

As mentioned earlier, this report focuses largely on the cybersecurity regulatory framework among the federal banking regulators—the FDIC, the OCC, and the Federal Reserve—as well as the NCUA and the CFPB. Together these agencies are responsible for implementing and ensuring compliance with banking laws.

Generally, banking institutions are regulated by a primary federal regulator (PFR). The PFR for each type of banking institution depends on its charter, as summarized in **Table 1**. In addition, the CFPB promulgates a number of consumer protection rules for a variety of financial institutions, including certain banks.

**Table 1. Regulatory Jurisdiction for Different Banking Institutions**

| Bank Charter Type | Primary Federal Regulator |
|---|---|
| State charter, member of Federal Reserve | Federal Reserve |
| State charter, nonmember | Federal Deposit Insurance Corporation |
| Federal charter | Office of the Comptroller of the Currency |
| Credit unions | National Credit Union Administration |

**Source:** CRS analysis.

**Note:** All national banks are also members of the Federal Reserve.

## GLBA Data Privacy and Safeguards

As mentioned above, GLBA provides the most comprehensive framework for cybersecurity regulation among financial institutions. While this section largely focuses on the GLBA provisions for regulating data privacy and security practices for banks, GLBA applies to a broad range of financial institutions.[14] This framework is built upon two pillars: (1) privacy standards that impose disclosure limitations concerning consumers' information, and (2) security standards that require institutions to implement certain practices to safeguard the information from unauthorized access, use, and disclosure. The two major rules for implementing this framework are known as the Privacy Rule (Regulation P) and the Safeguards Rule, respectively. Each rule is summarized below in **Table 2**.

[13] CQ Markup Report, H.R. 1165: Data Privacy Act, at https://plus.cq.com/bill/118/HR1165?3.

[14] Financial institutions are defined under P.L. 106-102 as any institution that engages in activities that are financial in nature. See 12 U.S.C. §6809.

**Table 2. Summary of Privacy and Safeguards Rules**

Requirements for Financial Institutions

| Privacy Rule | Safeguards Rule |
|---|---|
| • provide initial, annual, and revised privacy policy notices to customers; and<br>• set the conditions for when a financial institution may or may not disclose nonpublic personal information. | • design and implement a safeguards program; and<br>• identify and assess the risks to customer information in each relevant area of the company's operation, including service providers and changes in the firm's operations. |

**Source:** CRS analysis of relevant provisions of the Gramm-Leach-Bliley Act (P.L. 106-102).

These rules are promulgated by several government agencies, and the regulators generally have supervisory and enforcement authority over the entities in their jurisdiction. This is shown in **Table 3** and **Table 4**.

## GLBA Rulemaking Authorities

Rulemaking authority to implement the Privacy Rule through Regulation P is vested in four agencies. The CFPB promulgates the Privacy Rule for banks. The Federal Trade Commission (FTC) has the rulemaking authority for the Safeguards Rule. **Table 4** provides an overview of federal agencies with GLBA rulemaking authority and which entities they regulate under each rule.

**Table 3. Relevant Rulemaking Authority for GLBA**

| Federal Regulator | Privacy Rule | Safeguards Rule |
|---|---|---|
| Consumer Financial Protection Bureau (CFPB) | Depository and nonbank financial institutions involving consumer financial products or services in the CFPB's jurisdiction | None |
| Federal Trade Commission (FTC) | n/a | Financial institutions significantly engaged in financial activities (e.g., bank and nonbank lenders, real estate appraisers, professional tax preparers, courier services, credit reporting agencies, and ATM operators) |

**Sources:** 15. U.S.C. §6804; 12 C.F.R. §1016.1(b).

## Recent Updates on Depository Regulation of GLBA Cybersecurity Provisions

Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank; P.L. 111-203) transferred rulemaking authority for most provisions of Subtitle A of Title V of GLBA to the CFPB. As can be seen in more detail in the following section, Dodd-Frank also granted authority to the CFPB to examine and enforce compliance with respect to entities, including banks, under its jurisdiction.[15] In December 2011, the CFPB effectively recodified Regulation P in Title 12, Part 1016, of the *Code of Federal Regulations*.[16] The most recent

[15] CFPB, *Laws and Regulations*, "GLBA Privacy," October 2016, at https://files.consumerfinance.gov/f/documents/102016_cfpb_GLBAExamManualUpdate.pdf.

[16] See CFPB, "Privacy of Consumer Financial Information (Regulation P)," 76 *Federal Register* 79025, December 21,

amendment to its rulemaking occurred in 2018, when a 2015 statutory amendment from the Fixing America's Surface Transportation (FAST Act; P.L. 114-94) provided an exception to the annual notice requirement for financial institutions that meet certain conditions.[17]

The FTC codified its implementation of the Safeguards Rule in 2002 in Title 16, Part 314, of the *Code of Federal Regulations*.[18] In 2016, the FTC sought public comments on the Safeguards Rule to assess the economic impact and benefits of the rule; possible conflict between the rule and state, local, or other federal laws or regulations; and the effect on the rule of any technological, economic, or other industry changes.[19]

On October 27, 2021, the FTC announced that it had issued a new final rulemaking[20] to specify safeguards financial institutions must implement as part of their information security programs—including limiting who can access consumer data and requiring encryption to secure the data. Under the updated Safeguards Rule, institutions must also explain the administrative, technical, and physical safeguards used to "access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle" customer information. Further, the definition of *financial institution* was expanded to include institutions that charge fees to connect consumers to potential lenders. In addition, the rule requires a financial institution to designate a single qualified individual to oversee its information security program and provide periodic reports to the institution's board or information security officials. The FTC also announced that it is seeking comment in a supplemental notice of proposed rulemaking on an additional change to the Safeguards Rule to require financial institutions to report certain data breaches and other security events to the FTC.[21]

## Other Regulatory Developments

In November 2021, the OCC, Federal Reserve, and FDIC announced a joint final rulemaking that imposed rapid notification requirements on banking organizations and bank service providers following "significant" computer-security incidents.[22] The rule requires a financial institution to notify its supervisor as soon as possible and no later than 36 hours after the banking organization believes in good faith that the incident occurred. This notification requirement is intended to serve as an early alert to a banking organization's primary federal regulator and is not meant to provide an assessment of the incident. Additionally, a bank service provider is required to notify each affected banking organization customer immediately after the provider experiences a computer security incident that has caused or is likely to cause a material service disruption for four or more hours.

---

2011.

[17] CFPB, "Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act (Regulation P)," 83 *Federal Register* 40945, August 17, 2018.

[18] See FTC, "Standards for Safeguarding Customer Information," 67 *Federal Register* 36484, May 23, 2002.

[19] See FTC, "Standards for Safeguarding Customer Information," 81 *Federal Register* 61632, September 7, 2016.

[20] See FTC, "Standards for Safeguarding Customer Information," 86 *Federal Register* 70272-70314, December 9, 2021.

[21] See FTC, "Standards for Safeguarding Customer Information," 86 *Federal Register* 70062-70067, December 9, 2021.

[22] OCC, Federal Reserve, and FDIC, "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers," 86 *Federal Register* 66444, November 23, 2021 at https://www.federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank.

# Supervisory Process

In addition to writing rules to implement provisions of law, banking regulators have authority to conduct examinations or supervise institutions in their jurisdiction to ensure they are complying with the rules. As noted earlier, cybersecurity threats pose operational risk, reputational risk, and potentially systemic risk. Banking regulators together monitor these risks through the Federal Financial Institutions Examination Council (FFIEC).[23] FSOC monitors systemic risks to the financial system, including cyber threats. The FFIEC coordinates bank examinations for safety and soundness, as well as for compliance and information technology. Further, bank partnerships with third-party service providers are subject to the supervisory processes set forth in the BSCA.

## GLBA Supervision

Agencies responsible for privacy and safeguard rulemaking are sometimes not the same agencies responsible for implementing and enforcing these rules for a particular entity. For instance, while the FTC has rulemaking authority for the Safeguards Rule, the banking and credit union regulators share supervisory authority for the rule. Further, most of the financial regulators have some supervisory or enforcement authority to ensure that the institutions in their respective jurisdictions comply with the Privacy and Safeguards Rules (see **Table 4**).

**Table 4. Supervision and Enforcement Authority for GLBA**

| Federal Regulator | Privacy Rule | Safeguards Rule |
|---|---|---|
| CFPB | Supervision and enforcement authority over depository and nonbank financial institutions involving consumer financial products or services in the CFPB's jurisdiction | None |
| Bank and Credit Union Regulators | Supervision and enforcement authority over banks or credit unions in their jurisdiction | Supervision and enforcement authority over banks or credit unions in their jurisdiction |

**Source:** 15 U.S.C. §6805.

**Note:** The depository agencies include the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Federal Reserve, and the National Credit Union Administration.

## Depository Institution Supervision

Bank and credit union regulators have dedicated teams of examiners who conduct both routine and special examinations of depository institutions to ensure that they are operating in a safe and sound manner, complying with relevant laws, and maintaining adequate information technology systems. Each of the regulators inform the financial institutions under their jurisdiction about their supervisory expectations. In addition, while the regulatory framework for banks and credit unions is complex and fragmented among several agencies, the examination procedures among these agencies are largely coordinated through the FFIEC.

The depository regulators each approach cybersecurity examinations and supervision in different ways. **Table 5** illustrates the general approaches and resources that each agency has established

[23] Federal Reserve, FDIC, NCUA, OCC, and the CFPB, along with representatives from state supervising organizations, comprise FFIEC.

with respect to cybersecurity and information security. While each agency has developed its own approaches, tools, and resources, each agency relies on the FFIEC resources as well. The basic approaches include providing guidance to industry on how certain activities will be treated, policy manuals and handbooks that lay out the guidelines for examinations, and technical assistance.

**Table 5. Depository Supervision Toolkit for Cybersecurity**

| Agency | Supervisory Approaches & Resources | FFIEC Resources for Examinations |
|---|---|---|
| NCUA | Automated Cybersecurity Evaluation Toolbox<br>Examinations (NCUA Examinations Guidebook and FFIEC Handbook)<br>National Supervision Policy ManualGuidance<br>Letters to Credit Unions<br>Risk Alerts | |
| FDIC | Examinations for IT (IT Risk Management Program and FFIEC Handbook)<br>Technical Assistance Video Series<br>Supervisory Insights Journal<br>Cyber Challenge for Community Banks<br>Guidance (FDIC Financial Institution Letters) | IT Examination Handbook<br>Cybersecurity Assessment Tool<br>IT and Related Guidance |
| OCC | Examinations for IT (FFIEC Handbook and Comptroller's Handbook for Bank Supervision)<br>Guidance (OCC Bulletins) | |
| Federal Reserve | Examinations for IT (Commercial Bank Examination Manual and FFIEC Handbook)<br>Policy Letters (Supervision and Regulation Letters) | |

**Source:** CRS analysis of each agency's cybersecurity, IT, and examination websites.

**Notes:** Intended for illustrative purposes only; not intended to capture all measures taken by an agency. Regulatory resources for information on these supervisory programs can be found at https://ithandbook.ffiec.gov/it-booklets.aspx; https://www.fdic.gov/resources/bankers/information-technology/; and https://ncua.gov/regulation-supervision/regulatory-compliance-resources/cybersecurity-resources/ncuas-information-security-examination-and-cybersecurity-assessment.

## Third-Party Service Providers

As banks facilitate more transactions through digital channels, financial institutions are increasingly relying on third-party vendors, specifically technology service providers (TSPs), to provide software and technical support. In light of this development, regulators are scrutinizing how banks manage their *operational risks*.[24] Rising operational risks—particularly cyber risks (e.g., data breaches, insufficient customer data backups, and operating system hijackings)—have compelled regulators to scrutinize banks' security programs. Regulators require an institution that uses a TSP to ensure that the TSP performs in a safe and sound manner, and activities performed by a TSP for a bank must meet the same regulatory requirements as if they were performed by the bank itself.

The BSCA gives regulators a broad set of authorities to supervise TSPs that have contractual relationships with banks. The BSCA directs the regulators to treat all activities performed by contract as if they were performed by the bank and grants them the authority to examine and

[24] See Basel Committee on Banking Supervision, *Principles for the Sound Management of Operational Risk*, June 2011, at https://www.bis.org/publ/bcbs195.pdf.

regulate third-party vendors that provide services to banks, including check and deposit sorting and posting, statement preparation, notices, bookkeeping, and accounting.

The banking regulators issued interagency guidelines in 2001 regarding information security programs. The guidance requires banks to provide continuous oversight of third-party vendors such as TSPs. The regulators periodically update guidance and have since released additional guidance pertaining to third-party vendors.[25] For example, the Federal Reserve, FDIC, and OCC have each issued guidance addressing third-party relationships and appropriate risk management practices in 2008 and 2013, respectively.[26] In July 2021, the FDIC, Federal Reserve, and OCC issued joint proposed guidance on third-party relationships.[27] The proposed guidance assists banking organizations in managing third-party relationships. Further, in August 2021, the OCC issued guidance on financial technology third-party relationships.[28]

# Policy Issues for Congress

Oversight of financial services and bank cybersecurity reflects a complex and sometimes overlapping array of state and federal laws, regulators, regulations, and guidance—many of which predate the emergence of cybersecurity risk. Whether this framework provides adequate protection against cyberattacks without imposing undue cost burdens on banks is an open question. Successful hacks of banks and other financial institutions, in which large amounts of personal information were stolen or compromised, highlight arguments about the importance of ensuring bank cybersecurity.

That several regulators implement, supervise, and enforce federal provisions has also raised questions over the patchwork nature of regulatory standards for consumer privacy and security. With so many agencies involved with the cybersecurity of financial institutions, the Government Accountability Office (GAO) has raised concerns over interagency cooperation and tracking the success of agency efforts.[29] Some argue that a unified and modernized legislative framework could improve this patchwork approach.

As Congress continues to explore this issue, a few policy considerations, detailed below, may be informative.

---

[25] For example, see the following releases: NCUA, *Evaluating Third Party Relationships*, Letter No.: 07-CU-13, December 2007; FDIC, *Guidance for Managing Third-Party Risk*, FIL-44-2008, June 6, 2008; FFIEC, "Financial Regulators Release Guidance for the Supervision of Technology Service Providers," press release, October 31, 2012, at https://www.ffiec.gov/press/pr103112.htm; FDIC, *Technology Outsourcing: Informational Tools for Community Bankers*, FIL-13-2014, April 7, 2014; FDIC Office of Inspector General, *Technology Service Provider Contracts with FDIC-Supervised Institutions*, Office of Audits and Evaluations, Report No. EVAL-17-004, February 2017; and NCUA Office of Inspector General, *Audit of the NCUA Information Technology Examination Program's Oversight of Credit Union Cybersecurity Programs*, Report No OIG-17-08, September 28, 2017.

[26] For example, see FDIC, "Guidance for Managing Third-Party Risk," June 6, 2008, at https://www.fdic.gov/news/financial-institution-letters/2008/fil08044.html; Federal Reserve, "Guidance on Managing Outsourcing Risk," December 5, 2013 (revised February 26, 2021), at https://www.federalreserve.gov/supervisionreg/srletters/sr1319.htm; and OCC, "Third-Party Relationships: Risk Management Guidance," October 30, 2013, at https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

[27] Federal Reserve, FDIC, and OCC, "Proposed Interagency Guidance on Third-Party Relationships: Risk Management," July 13, 2021, at https://www.fdic.gov/news/financial-institution-letters/2021/fil21050.html.

[28] OCC, "OCC Bulletin 2021-40," August 27, 2021, at https://www.occ.gov/news-issuances/bulletins/2021/bulletin-2021-40.html.

[29] U.S. Government Accountability Office, *Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts*, GAO-20-631, September 17, 2020, https://www.gao.gov/products/gao-20-631.

## Data Privacy

GLBA's financial data privacy provisions covers only nonpublic personal information held by financial institutions significantly engaged in financial activities. However, as the industry's data use has grown, some have debated whether the law covers all sensitive individual financial information. For example, data brokers can compile public and private data from different sources, many of which may not be subject to GLBA's provisions; combining these data might reveal financially sensitive information about a consumer. Further, consumers have a limited ability to know, control, or correct financial data, which can make it difficult to obtain redress for violations such as data breaches.

## Technology Service Providers

Regulation aimed at banks' relationships with third-party vendors such as TSPs has benefits in mitigating operational risks but also imposes costs on banks. Some banks, particularly community banks and small credit unions, may find it difficult to comply with regulatory standards applicable to their relationship with third-party vendors. For example, certain institutions may be unable to conduct appropriate due diligence when selecting TSPs or to structure contracts that adequately protect against potential TSPs-related risks. Some banks may also lack the resources to monitor whether the TSPs are adhering to GLBA and other regulatory or contract requirements. Regulatory compliance costs are sometimes cited as a factor in banking industry consolidation, because compliance costs may be subject to economies of scale that incentivize small banks to merge with larger ones or other small banks to combine their resources to meet their compliance obligations.[30]

### Cloud Computing

Financial institutions may outsource the management of different controls over information assets and operations to cloud service providers (CSPs).[31] Banks pay CSPs to use their computing resources (e.g., servers and mainframes), rather than purchasing and maintaining their own. This relationship is referred to as a shared responsibility model, in which banks and CSPs are responsible for discrete tasks of a shared work stream. Failure to implement an effective risk management process could put sensitive information at risk.

The BSCA gives bank regulators supervisory authority over service providers.[32] Exercising this authority over CSPs, however, may raise challenges. Despite the integration of cloud services by the banking industry, different expectations from bank regulators and the cloud service industry,—such as what to expect during bank-like examinations—may persist.

Large, systemically important banks are reportedly moving significant portions of their operations onto cloud services, which could exacerbate the effects of a disruption at a CSP.[33] The cloud market is concentrated in three major CSPs—Amazon Web Services, Microsoft Azure, and

[30] For more information on banking industry consolidation, see CRS In Focus IF11956, *Bank Mergers and Acquisitions*, by Marc Labonte and Andrew P. Scott.

[31] For more on bank use of cloud technology, see CRS In Focus IF11985, *Bank Use of Cloud Technology*, by Paul Tierno.

[32] 12 U.S.C. §1867(c).

[33] Ibid.

Google Cloud—that collectively account for between 60%[34] and 70%[35] of market share and perhaps more among banks. In its 2022 annual report, FSOC identified "the financial sector's concentrated dependency on a limited number of service providers, such as cloud service providers, for critical information technology services as a potential risk to financial stability."[36] Traditional bank risks such as market and liquidity risks—not normally cloud computing concerns—can arise if the banks' abilities to transact are impeded by cloud-related disruptions. Banking regulators are concerned with risks to financial stability, so policymakers may choose to consider whether their authorities to regulate CSPs are appropriately calibrated.

Considering this close relationship, the scope of bank supervision may expand to CSPs. This may lead to technical resource mismatches, and regulators, like banks,[37] may find themselves with a shortage of cloud skills necessary to examine CSPs. CSPs may also not be familiar with or amenable to audits or bank-like examinations.[38] The Federal Reserve Bank of Richmond performed a formal exam of Amazon Web Services in April 2019, which reportedly exposed this culture clash.[39] Close integration between banks and CSPs may accelerate regulators' call for regular examination of CSPs to monitor aspects of their relationships with banks, including security and financial system stability risks.

Obstacles to data portability, such as proprietary technology and restrictive vendor contracts, may make switching CSPs difficult. Therefore, banks may adopt multi-cloud strategies—contracts with multiple CSPs—to avoid lock-in risk.[40] In addition to increasing costs, this introduces potentially two or more providers in the form of CSPs, and banks must manage these relationships effectively to ensure cybersecurity.

## Author Information

Andrew P. Scott
Analyst in Financial Economics

Paul Tierno
Analyst in Financial Economics

[34] Felix Richter, "Amazon Leads $150-Billion Cloud Market," *Statista*, July 5, 2021, at https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/.

[35] Gartner, "Gartner Says Worldwide IaaS Public Cloud Services Market Grew 40.7% in 2020," press release, June 28, 2021, at https://www.gartner.com/en/newsroom/press-releases/2021-06-28-gartner-says-worldwide-iaas-public-cloud-services-market-grew-40-7-percent-in-2020.

[36] FSOC, *2022 Annual Report*, December 16, 2022, p. 70, at https://home.treasury.gov/system/files/261/FSOC2022AnnualReport.pdf.

[37] Abbott, Michael, "Challenges and Opportunities in Banks' Cloud Migration," Accenture, January 27, 2021, at https://bankingblog.accenture.com/challenges-opportunities-banks-cloud-migration.

[38] Penny Crossman, "Timely Reminder About Who Bears Responsibility For Cloud Security," *American Banker*, May 4, 2020, at https://www.americanbanker.com/news/timely-reminder-about-who-bears-responsibility-for-cloud-security.

[39] Liz Hoffman, Dana Mattioli, and Ryan Tracy, "Fed Examined Amazon's Cloud in New Scrutiny for Tech," *The Wall Street Journal*, August 1, 2019, at https://www.wsj.com/articles/fed-examined-amazons-cloud-in-new-scrutiny-for-tech-11564693812.

[40] Matthew Leybold, Hrishi Hrishikesh, and Benjamin Rehberg, "Financial Institutions Need to Pursue Their Own Path to the Cloud," BCG, May 5, 2021, at https://www.bcg.com/publications/2021/strategies-for-financial-institutions-transitioning-to-the-cloud.

## Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.