MAXINE WATERS, CA
CHAIRWOMAN

United States House of Representatives
Committee on Financial Services
2129 Rayburn House Office Building
Washington, D.C. 20515

PATRICK MCHENRY, NC
RANKING MEMBER

October 29, 2021

Memorandum

To: Members, Committee on Financial Services
From: FSC Majority Staff
Subject: November 3, 2021, Subcommittee on Consumer Protection and Financial Institutions hearing entitled, "Cyber Threats, Consumer Data, and the Financial System"

The Subcommittee on Consumer Protection and Financial Institutions will hold a hearing entitled, "Cyber Threats, Consumer Data, and the Financial System" on Wednesday, November 3, 2021 at 10 a.m. in room 2128 of the Rayburn House Office Building and on the Cisco Webex platform. This hearing will have one panel with the following witnesses:

- **Samir Jain**, Director of Policy, Center for Democracy & Technology
- **Robert E. James, II**, President & CEO, Carver Financial Corporation
- **Carlos Vazquez**, Chief Information Security Officer, Canvas Credit Union
- **Jeff Newgard**, President and Chief Executive Officer, Bank of Idaho, on behalf of the Independent Community Bankers of America

Overview

According to a recent report, a critical cyberattack on a large, systemically important company or regional utility could create economic losses greater than a major natural disaster.[1] The financial services sector is a top target for cybercriminals seeking to steal financial assets, consumer and business data, or deploy ransomware, disrupt services, and shut down networks.[2] According to financial regulators, cyber threats are increasingly more sophisticated, organized, and a growing area of concern.[3] Major financial companies agree. Testifying before the House Financial Services Committee in May 2021, when asked what they see as the "greatest threat to our financial system right now," four of the six CEOs of the largest U.S. banks' responses included cybersecurity.[4] Cyberattacks on banks are also increasing in number. Through the first half of 2021, banks and credit unions experienced a 1,318% increase in ransomware attacks.[5] According to one study, the likelihood of cybercrime being detected, reported, and enforcement action taken may be as low as 0.05%.[6] This hearing will examine cybersecurity and consumer data protection challenges for financial institutions, efforts by the U.S. Department of Treasury (Treasury Department) and other government agencies to strengthen cyber defenses in the financial sector, and review the current legal framework governing data security.

---

[1] FDD, Intangic, The Economic Costs of Cyber Risk, (June 28, 2021).
[2] *See* Forbes, Cybercrime: 25% Of All Malware Targets Financial Services, Credit Card Fraud Up 200%, (Apr. 29, 2019); *See also* Business Wire, COVID Cyber Crime: 74% of Financial Institutions Experience Significant Spike in Threats Linked To COVID-19, (Apr. 28, 2021).
[3] Federal Reserve, Report to Congress: Cybersecurity and Financial System Resilience Report, p. 20, (Sept. 2021); Testimony of Michael Hsu, Acting Comptroller of the Currency before the Committee on Financial Services, (May 19, 2021).
[4] Committee, Hearing entitled, Holding Megabanks Accountable: An Update on Banking Practices, Programs and Policies, (May 27, 2021).
[5] Security Magazine, Banking industry sees 1318% increase in ransomware attacks in 2021, (Sept. 20, 2021).
[6] Third Way, To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors, (Oct. 29, 2018).

Cybersecurity and Consumer Data Laws

Federal policy governing cybersecurity and data protection for financial institutions is often intertwined and spread across several laws, rules, and agencies. Additionally, as businesses collect more sensitive data from consumers, consumers face an increasing risk that their data will be lost, mishandled, or stolen.[7] The Gramm-Leach-Bliley Act of 1999 (GLBA), the most comprehensive federal law on privacy and data security for financial institutions, directs financial regulators to institute a framework for consumer data privacy and security safeguards.[8] Title V, Subtitle A of GLBA limits financial institutions from sharing nonpublic consumer data with unaffiliated third parties, requires financial institutions to disclose privacy policies to consumers and authorizes regulators to promulgate regulations.[9] Title X of the Dodd-Frank Act Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) transferred rulemaking authority of consumer data privacy protections under GLBA to the Consumer Financial Protection Bureau (CFPB), which subsequently reissued rules under Regulation P.[10] The enforcement powers under Regulation P are shared among the federal banking regulators, the Federal Trade Commission (FTC), the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), and the state insurance commissioners.[11]

Under GLBA's data security provision, the financial regulators (except the CFPB) and FTC have promulgated versions of the Safeguards Rule.[12] By statute, these rules require regulators to "establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards— (1) to ensure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[13]

Other laws also include cybersecurity and data privacy provisions. Under the Sarbanes-Oxley Act of 2002, public companies, foreign and domestic private issuers, and issuers of asset-backed securities must disclose internal and external risks and how they respond to such risks in reports filed with the SEC.[14] The SEC has interpreted such risks to be inclusive to cybersecurity.[15] The Fair and Accurate Credit Transactions Act of 2003 (FACT Act) amended the Fair Credit Reporting Act (FCRA) to require regulatory agencies to develop identity theft protocols such as allowing consumers to use fraud alerts on their credit files.[16] Additionally, the Electronic Fund Transfer Act (EFTA) requires financial institutions conducting electronic fund transfer services to disclose certain information to consumers, including when a financial institution may share data with a third party.[17]

Recent Actions Regarding Consumer Data

---

[7] *See* Deloitte, The Deloitte Consumer Review - Consumer data under attack: the growing threat of cyber crime, (Nov. 2015).
[8] P.L. 106-102; *See also* CRS, Financial Services and Cybersecurity: The Federal Role, R44429, (Updated Mar. 23, 2016).
[9] *Id.*
[10] CFPB, 12 CFR Part 1016 - Privacy of Consumer Financial Information (Regulation P), (Most recently amended Sept. 17, 2018).
[11] P.L. 106-102.
[12] CRS, Financial Services and Cybersecurity: The Federal Role, R44429, (Updated Mar. 23, 2016).
[13] P.L. 106–102; 15 USC 6801.
[14] P.L. 107-204.
[15] *See* SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, (Feb. 21, 2018).
[16] P.L. 108-159 §§114 and 216. 15 U.S.C. §1681m and 15 U.S.C. §1681w.
[17] CFPB, 12 CFR Part 1005 (Regulation E).

The CFPB is currently engaged in multiple issues regarding consumer data and privacy. In November 2020, the CFPB issued an Advanced Notice of Proposed Rulemaking (ANPR) to implement Section 1033 of the Dodd-Frank Act, which ensures consumer access to their financial data in the possession of a financial institution.[18] Prior to the ANPR's release, the CFPB requested stakeholder feedback and information on consumer data sharing between financial institutions, which resulted in a report outlining nine principles, based in part on the feedback.[19] On July 9, 2021, President Biden signed Executive Order 14036, "Promoting Competition in the American Economy," which, among other things, directed the CFPB to issue rules under Section 1033 of the Dodd-Frank Act. Additionally, on October 21, 2021, the CFPB issued orders to collect information from large tech companies operating payments systems in the U.S. to "better understand how these firms use personal payments data and manage data access to users so the Bureau can ensure adequate consumer protection."[20]

Moreover, on October 27, 2021, the FTC updated its Safeguards Rule pursuant to GLBA to require non-bank financial institutions to have a comprehensive security system to keep their customers' information safe. The updated rule requires financial institutions to, among other things, use encryption to better secure data.[21]

Gaps in Regulatory Oversight

Financial institutions often and increasingly rely on technology service providers and other vendors for technical expertise and other business services.[22] In some cases, vendors may lack experience with financial regulation compliance, potentially introducing additional cybersecurity risks.[23] According to a recent report from VMware, "38 percent of surveyed financial institutions said they've encountered island hopping, an attack where supply chains and partners are commandeered to target the primary financial institution." The SolarWinds cyberattack is one example of network-based "island hopping."[24] Ransomware attacks, phishing, and other cyberattacks often target financial institutions' service providers to reach their true target—financial institutions and their customers.[25]

The Bank Service Company Act of 1962 authorizes the Federal Reserve, OCC, and FDIC to examine and regulate companies providing certain services to banks as if the bank were performing the service itself.[26] However, the NCUA lacks this authority of credit union service organizations (CUSOs).[27] The agency had been granted temporary authority to examine third-party firms related to the Y2K computer issue, but that authority expired in 2002.[28] The NCUA, the Financial Stability Oversight Council

---

[18] Federal Register, Consumer Access to Financial Records, CFPB-2020-0034, (Nov. 6, 2020).
[19] *See* CFPB, Consumer-authorized financial data sharing and aggregation, (Oct. 18, 2017); See also CFPB, Consumer-Authorized Financial Data Sharing and Aggregation: Stakeholder Insights That Inform the Consumer Protection Principles (Oct. 18, 2017).
[20] CFPB, CFPB Orders Tech Giants to Turn Over Information on their Payment System Plans, (Oct. 21, 2021).
[21] FTC, FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches (Oct. 27, 2021).
[22] *See CRS,* Fintech: Overview of Innovative Financial Technology and Selected Policy Issues, R46332, (Apr. 28, 2020); See also FSOC, 2020 Annual Report, (December 2020), p.8-9.
[23] *See* Fed, FDIC, OCC, Proposed Interagency Guidance on Third-Party Relationships: Risk Management, (Jul. 13, 2021).
[24] *Id.*
[25] VMware, Modern Bank Heists 4.0, (Apr. 13, 2021).
[26] P.L. 87-856. 12 U.S.C. §§1861-1867; *See also* CRS, Financial Services and Cybersecurity: The Federal Role, R44429, (Updated Mar. 23, 2016).
[27] NCUA Office of the Inspector General, Audit of the NCUA's Examination and Oversight Authority over Credit Union Service Organizations and Vendors, (Sept. 1, 2020).
[28] Testimony of The Honorable Todd Harper, Chairman, National Credit Union Administration, before the Committee (May 19, 2021).

(FSOC), and the Government Accountability Office have requested this authority be restored.[29] Similarly, the Federal Housing Finance Agency (FHFA) lacks the authority to regulate Fannie Mae and Freddie Mac (GSEs) vendors.[30] According to the FHFA Office of the Inspector General, "[GSE] reliance on third-parties exposes them to various risks, including counterparty, operational, cyber, and reputational risks."[31]

Types of Cyberattacks

Financial institutions face a variety of different cyber threats.[32] *Ransomware*, which has exploded in use over the last years, is software designed to deny access to a computer system or data until a ransom is paid.[33] According to Suspicious Activity Report data collected by the Financial Crimes Enforcement Network (FinCEN), about $590 million in ransom was paid out in just the first six months of 2021, compared with $416 million paid in 2020 overall.[34] A *denial-of-service (DoS)* or *distributed denial-of-service (DDoS)* attack occurs when one or multiple machines disrupt the service of a computer or network, preventing legitimate users from accessing services.[35] *Malware* is software intended to gain access or cause damage to a computer or network, often while the victim or system remains oblivious to the fact there's been a compromise.[36] *Business Email Compromise (BEC)* is the use of social engineering to craft email messages that appear to come from familiar sources making legitimate requests such as a money transfer or access to a computer network.[37] *Phishing* is the use of email or text messages designed to trick the victim into giving personal information that allows the criminal to steal passwords, account numbers, Social Security numbers, and access to email, bank, or other accounts.[38] *Man-in-the-Middle Attacks* can be characterized as "cyber eavesdropping on conversations between two parties and intercept data through a compromised but trusted system."[39]

Systemic Risk from Cyberattacks

Cyber threats also constitute systemic risks. The FSOC has consistently identified cybersecurity as a systemic risk in its annual reports to Congress.[40] In its 2020 Annual Report, FSOC highlighted an elevated cyber risk environment due in part to the COVID-19 pandemic and increased telework relying on less secure home networks.[41] Additionally, a recent report from the Federal Reserve Bank of New York found that if a cyberattack impaired any one of the five most active banks in the wholesale payments network, this "would result in significant spillovers to other banks, with 38 percent of the network affected on average" and that 6 percent of affected institutions would experience a detrimental gap in reserves.[42] The same report highlighted the consequences for nearly 10 percent of U.S. metropolitan statistical areas (MSAs), which would experience serious disruptions if one of the largest banks were attacked, especially areas where large amounts of consumer deposits are held by the financial institutions which are more

---

[29] *Id.*
[30] FHFA OIG, Enterprise Third-Party Relationships: Risk Assessment and Due Diligence in Vendor Selection, WPR-2020-003, (Mar. 12, 2020).
[31] *Id.*
[32] *See* HUB Security, Top Cyber Threats Facing Banks in 2021, (Feb. 2, 2021); *See also* Allianz Global Corporate & Specialty, Financial Services risk: Cyber security concerns grow, (May 2021).
[33] CISA, Ransomware 101, (Accessed Oct. 24, 2021).
[34] FinCEN, Financial Trend Analysis: Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021, (Oct. 2021).
[35] CISA, Understanding Denial-of-Service Attacks, Security Tip (ST04-015), (Updated Nov. 2019).
[36] CISA, Handling Destructive Malware, Security Tip (ST13-003), (Feb. 1, 2021).
[37] FBI, Business Email Compromise, (Accessed Oct. 28, 2021).
[38] FTC, How to Recognize and Avoid Phishing Scams, (Updated May 2019).
[39] CSO, What is a man-in-the-middle attack? How MitM attacks work and how to prevent them, (Feb. 13, 2019).
[40] Treasury, FSOC Annual Reports Archive (Accessed Oct. 28, 2021).
[41] FSOC, 2020 Annual Report, (December 2020), p.8-9
[42] FRBNY, Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis, No. 909, (Revised May 2021).

connected in the payment system. Additionally, the report highlighted the importance of and risk carried by third-party service providers, particularly for smaller banks using a common vendor.[43] Another analysis examining the potential for a bank run caused by panic induced by one or more cyberattacks on financial institutions also found a substantial risk to the payments system. It found "activity on the Automated Clearing House—which makes up more than half of all non-cash payment activity—is highly concentrated among a few member institutions. Were one of these nodes to be taken down, even for a short period of time, the economic impact could be significant."[44]

Financial Sector and Government Response to Cyber Threats

As more financial services are increasingly provided online, cyber defenses and responses to attacks have drawn the attention of governments and the financial services industry, where the cost of cybercrime per company is more expensive than any other industry.[45] In a survey of community bankers sponsored by the Conference of State Bank Supervisors and FDIC, nearly 71 percent of respondents listed cybersecurity as a significant risk—significantly higher than any other risk posed in the survey.[46] For the largest U.S. banks, cybersecurity efforts top more than $1 billion per year.[47] Additionally, new technologies, such as artificial intelligence have been increasingly employed by financial services providers to help assess suspicious patterns data more efficently. Financial regulators have been examining what benefits and risks these new technologies pose in cybersecurity.[48]

On May 12, 2021, President Biden issued Executive Order 14208, "Improving the Nation's Cybersecurity," to enhance information sharing between the government and private sector, modernize cybersecurity standards in the government, improve software supply chain security, establish a Cyber Safety Review Board, create a cyber incident response standard protocol, and improve investigative and remediation capabilities.[49] On September, 21, 2021, the Treasury Department announced several efforts to counter ransomware and disrupt cybercriminal networks.[50] The announcement detailed the Office of Foreign Assets Control's (OFAC) sanctions designation of a cryptocurrency exchange "for its part in facilitating financial transactions for ransomware actors," updated guidance on "Potential Sanctions Risk for Facilitating Ransomware Payments," and placed a heightened focus from FinCEN on ransomware.[51]

On September 23, 2021, the House of Representatives passed the National Defense Authorization Act for Fiscal Year 2022 which contained several provisions aimed at improving cyber defenses and responses.[52] The legislation would require Department of Homeland Security (DHS) and Cybersecurity and Infrastructure Security Agency (CISA) to establish requirements for critical infrastructure owners to report cybersecurity incidents to a newly created Cyber Incident Review Office within CISA.[53]

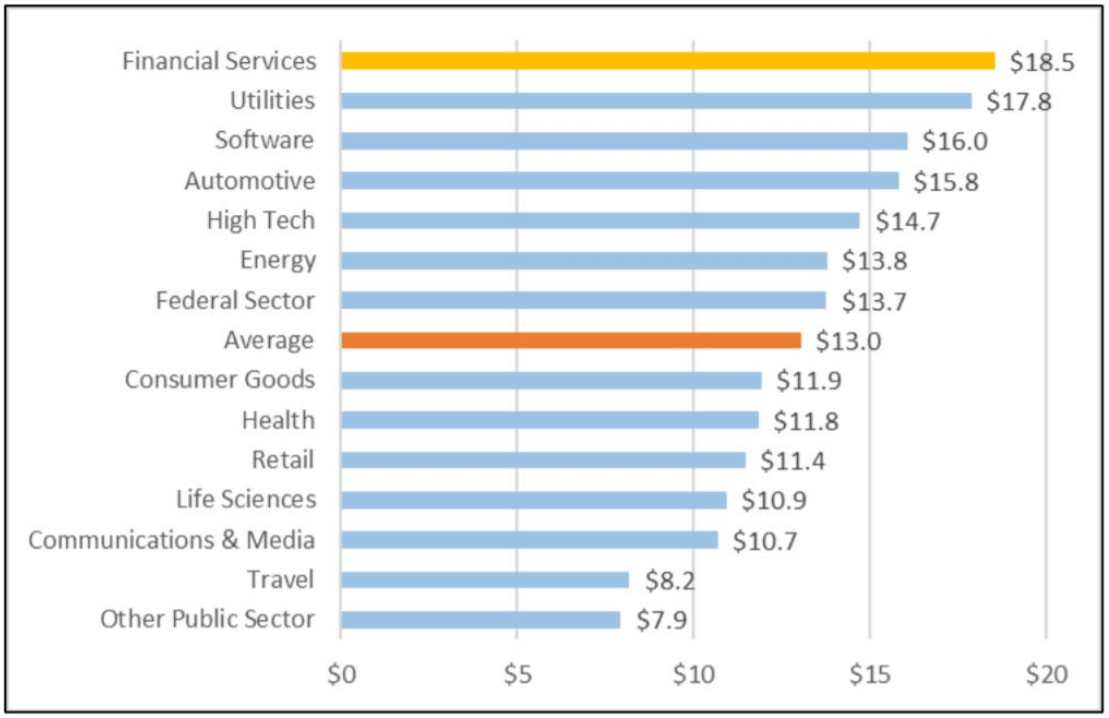
---

[43] *Id*. at 3.
[44] Brookings Institute, Cyber runs: How a cyber attack could affect U.S. financial institutions, (June 18, 2019).
[45] *See* American Banker, Cyberattacks draw tech, bank CEOs to White House for brainstorm, (Aug. 25, 2021); Figure 1.
[46] CSBS, FDIC, Community Banking in the 21st Century, 2019 Research and Policy Conference, (2019), p. 56-57.
[47] CNBC, Bank of America spends over $1 billion per year on cybersecurity, CEO Brian Moynihan says, (Jun. 14, 2021).
[48] For example, *see* CFPB, OCC, FDIC, Fed, and NCUA, Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning (Mar. 31, 2021).
[49] Executive Office of the President, Executive Order 14208, "Improving the Nation's Cybersecurity", (May 12, 2021).
[50] Department of Treasury, Treasury Takes Robust Actions to Counter Ransomware, Press Release, (Sept. 21, 2021).
[51] *Id.*
[52] H.R. 4350, National Defense Authorization Act for Fiscal Year 2022; *See also* House Committee on Homeland Security, House Passes Cyber Incident Reporting Legislation, Critical Cybersecurity and Homeland Security Provisions in NDAA, Press Release, Sept. 24, 2021.
[53] *Id.*

Appendix – Legislation

- **H.R. 3910, the Safeguarding Non-bank Consumer Information Act (Lynch),** which would clarify the Gramm-Leach-Bliley Act's consumer financial privacy and data security provisions and gives the CFPB rulemaking and enforcement authority over the safeguards rule with respect to data aggregators and other financial institutions.[54]
- **H.R.____, the Strengthening Cybersecurity for the Financial Sector Act (Foster),** which would reauthorize and make permanent authority NCUA had between 1998 and 2002 over credit union third-party vendors. The bill would also provide the Federal Housing Finance Agency with similar authority over third-party vendors of their regulated entities.
- **H.R. ____, the Enhancing Cybersecurity of Nationwide Consumer Reporting Agencies Act**, which would clarify that CFPB has authority to supervise and examine the nationwide CRAs – Equifax, TransUnion, and Experian – for cybersecurity, including compliance with GLBA's safeguard rule. The bill would also subject these CRAs to minimum cybersecurity training requirements, and require a CFPB study, in consultation with the Department of Homeland Security and other agencies, of recent data breaches of the nationwide CRAs and provide administrative and legislative recommendations to further enhance data security.[55]

Figure 1: Average Per-company Cost of Cybercrime Across Sectors (in millions)



Source: CRS, Introduction to Financial Services: Financial Cybersecurity, IF11717, (Jan. 4, 2021).

[54] For more information, see Committee Task Force on Financial Technology hearing, Banking on Your Data: the Role of Big Data in Financial Services (Nov. 21, 2019).

[55] For more information, see Committee hearing, Examining the Equifax Data Breach (Oct. 5, 2017); Committee, Continuation of hearing entitled "Examining the Equifax Data Breach" (Oct. 25, 2017); Committee hearing, Who's Keeping Score? Holding Credit Bureaus Accountable and Repairing a Broken System (Feb. 26, 2019); and Committee hearing, A Biased, Broken System: Examining Proposals to Overhaul Credit Reporting to Achieve Equity (Jun. 29, 2021).