Statement for the Record

On Behalf of the

American Bankers Association

Before the

Consumer Protection and Financial Institutions Subcommittee

Of the

House Financial Services Committee

November 3, 2021

American Bankers Association

Statement for the Record

On Behalf of the

American Bankers Association

Before the

Consumer Protection and Financial Institutions Subcommittee

Of the

House Financial Services Committee

November 3, 2021

Chairman Perlmutter and Ranking Member Luetkemeyer, thank you for the opportunity to submit this statement for the record on behalf of the members of the American Bankers Association (ABA)[1] for the hearing titled "Cyber Threats, Consumer Data, and the Financial System."

Banks are already subject to a wide-range of data protection, privacy and cybersecurity laws and regulations, and for many years have devoted the time, energy, and resources necessary to secure and protect data and earn the trust of our customers. ABA members are working hard to ensure that consumers remain protected from cyber-attacks, data breaches and other threats that put their sensitive personal and financial data at risk. These threats are constantly evolving and as consumers access a wide range and often novel financial services offerings, it is critical to ensure they retain the protections they have come to expect from their bank. Our statement summarizes current regulatory requirements that protect consumer data and privacy, our views on cybersecurity, and other threats to consumer data and makes several policy recommendations for Congressional and regulatory action to ensure that this data is protected going forward.

[1] The American Bankers Association is the voice of the nation's $22.8 trillion banking industry, which is composed of small, regional, and large banks that together employ more than 2 million people, safeguard nearly $19 trillion in deposits and extend $11 trillion in loans. Learn more at www.aba.com.

Overview

- GLBA and Data Privacy Protection. Banks are already subject to several data privacy laws and regulations, including Title V of the Gramm-Leach Bliley Act (GLBA). Any new legislation focusing on data privacy should take into consideration existing laws that apply to financial institutions and avoid new requirements that duplicate or are inconsistent with those laws, and should also preempt the existing patch-work of state data privacy laws.

- Cybersecurity. Our sector has devoted substantial time, energy, and resources to protecting our systems and consumer data. Cyber-enabled fraud and ransomware attacks are on the rise. Several bills have been introduced in the House and Senate requiring private sector entities to report significant cyber-attacks and ransomware payments to the Department of Homeland Security (DHS). Reporting such incidents is not enough, Congress should also ensure that the federal government and DHS effectively share threat information with the private sector on a timely basis and provide tools to help private entities mitigate the effects of the attacks and prevent future attacks.

- Data Aggregators. Consumer data is playing an ever-increasing role in all aspects of our economy. Section 1033 of the Dodd-Frank Act (DFA) guarantees consumers the right to access their financial data. Non-bank data aggregators hold a tremendous amount of consumer data. The Consumer Financial Protection Bureau (CFPB) has Section 1033 on its rulemaking agenda for 2022. Congress should urge the CFPB to bring non-bank data aggregators under its direct supervision.

- Payments. The financial marketplace has become a hotbed of innovation with new products and services being offered to consumers at an ever- accelerating pace. Monoline fintech firms, nonbank payment providers, large technology firms and decentralized finance technologies like cryptocurrency have entered the market and some are seeking access to the payments system, while seeking to avoid the full bank regulatory framework including data privacy and consumer protections. There should be

a high-bar for access to the payments system. Congress, the Federal Reserve Board, and other policy-makers should ensure that the stringent rules that apply to banks should be applied to any entity that offers bank-like products or services.

A. Banks and Financial Institutions Are Subject to Extensive Data Protection and Privacy Laws

Banks believe strongly in protecting consumers' sensitive personal and financial information and their privacy. For hundreds of years, customers have relied on banks to protect the privacy of their financial information. Because banks are literally at the center of people's financial lives, our industry has long been subject to federal and state data protection and privacy laws. For example, Title V of the Gramm-Leach-Bliley Act (GLBA) not only requires banks to protect the security and confidentiality of customer records and information, but it also requires banks to provide consumers with notice of their privacy practices and limits the disclosure of financial and other consumer information with nonaffiliated third parties.

In enacting the GLBA in 1999, Congress stressed how critical privacy and data security is within the financial industry.[2] In this regard, it was Congress' intent that a financial institution's privacy practices must be readily accessible and easy to understand ("transparent") so that consumers can make well-informed choices. For example, the GLBA requires banks to provide notice to their customers about their information collection policies and practices. The notice is required to be clear and conspicuous and accurately describe the consumer's right to opt-out of the sharing of personal information with non-affiliated third parties if the bank shares customer information with such parties outside of exceptions.

Most banks make their GLBA privacy notices easily accessible on their websites. In this regard, many banks provide these disclosures using a standardized model template issued by the Consumer Financial Protection Bureau (CFPB) that is designed to follow the same format used

[2] *See* 15 U.S.C. § 6801(a) (stating that "[i]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information").

for nutrition labeling on food products. The current disclosures for consumers were developed over years of effort by federal regulators and the industry. Similar transparency about data collection and information sharing that is provided by the financial sector should be available to consumers no matter the type of company with whom they do business. For purposes of Federal privacy legislation, the GLBA should be considered a tried-and-true model for transparency.

In addition to transparency, the GLBA generally prohibits a bank from providing customer information to a nonaffiliated third party unless the bank has provided the customer with notice and an opportunity to opt out and the customer has not elected to opt out of such sharing. In this regard, the GLBA contains carefully crafted exceptions to the limitations on disclosures to nonaffiliated third parties that are designed to ensure that financial markets, products, and services that depend on the flow of financial information function efficiently for the benefit of the consumer, the financial institution, and the financial markets generally. For example, the GLBA permits a bank to disclose customer information to a nonaffiliated third party "as necessary to effect, administer, or enforce a transaction that a consumer requests or authorizes" or in connection with "[s]ervicing or processing a financial product or service that a consumer requests or authorizes" or "[m]aintaining or servicing the consumer's account with" the bank. The exceptions are also designed to ensure that banks can comply with other legal and regulatory mandates and be able to share information to prevent fraud and illicit finance. Notwithstanding these exceptions, the GLBA generally prohibits a bank from disclosing a customer's account number or similar form of access number or access code for a consumer's credit card account, deposit account, share account, or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through e-mail.

The GLBA also required the federal regulatory agencies to establish standards for safeguarding customer information. These standards require financial institutions to ensure the security and confidentiality of customer information, protect against any anticipated threats to such information, and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. And, since April 1, 2005, the federal banking agencies have required banks to have in place incident response programs to address security incidents involving unauthorized access to customer information, including notifying customers of possible breaches when appropriate.

Banks also are subject to other, decades-old federal financial privacy and data protection laws, including the Fair Credit Reporting Act (FCRA) and the Right to Financial Privacy Act (RFPA). The FCRA, among other things, restricts the collection, use and sharing of information that is used to determine a consumer's eligibility for, among other things, credit, insurance, or employment. The FCRA functions to limit the extent to which affiliated financial institutions may share with each other information relating to consumers, including requiring notice and an opportunity to opt out before sharing non-transaction or non-experience information (*e.g.*, application information) that is used to determine eligibility for credit. Even to the extent that the FCRA permits affiliated financial institutions to share consumer information (*e.g.*, pursuant to notice and an opportunity to opt out), the FCRA limits the use of certain information for marketing if the information is received from an affiliate, including requiring notice and an opportunity to opt out before using the information for marketing purposes.

The RFPA protects individuals against unwarranted searches of personal financial records by the federal government. For example, a bank may not provide a federal government entity with access to copies of or the information contained in a customer's financial records except as permitted by the RFPA (*e.g.*, in response to a search warrant). Most states have similar laws limiting the disclosure of financial records to state government entities.

In addition, depending on their specific activities, a bank may be subject to a host of other federal privacy laws, including the Health Insurance Portability and Accountability Act, the Children's Online Privacy Protection Act, the CAN-SPAM Act, the Telephone Consumer Protection Act, the Electronic Communications Privacy Act, and the Driver's Privacy Protection Act, among others.

Banks are also subject to strict regulatory oversight and regular exams regarding their compliance with data protection and privacy laws. This oversight includes the Federal Financial Institutions Examination Council Information Technology Examination Handbook, which is an extensive document with over 1,000 pages of IT guidance and examination instructions used by banking regulators to measure compliance with IT governance and information security program management.

B. Data Privacy Legislation

Congress has long recognized the importance of privacy for financial institutions and put into place a regulatory framework of strong privacy protections balanced with commonsense exceptions to minimize marketplace disruptions while maintaining a high level of consumer safeguards. These protections have been buttressed by a number of other laws with strong privacy protections, and banks and their federal and state regulators work aggressively to ensure consumers remain strongly protected.

We believe that Title V of the GLBA played a critical role in the development of privacy legislation in this country. The GLBA represented this country's first effort to regulate the privacy practices of a specific sector and should be recognized as an important benchmark. Moreover, the GLBA contributed to ensuing development of other sector-specific federal laws (e.g., HIPAA) and broader state data protection laws, particularly breach notification and data security.

Given the passage of time and even recent state efforts to adopt generally applicable privacy legislation, it is fair to at least question whether the GLBA should be updated. It is noteworthy that each of the new state privacy laws (*e.g.*, California, Colorado, and Virginia) includes an exception for entities covered by the GLBA.[3] However, if Congress considers a "refresh" of the GLBA, it is critical to consider the potential unintended consequences to the financial system, accounts, and transactions. This is what Congress did in 1999 by ensuring that well-crafted exceptions were in place to allow financial institutions to disclose customer information in order to process transactions and to fight fraud. In new data privacy legislation, Congress should carefully consider whether any specific privacy right (beyond those already included in the GLBA) are appropriate with respect to the types of information that financial institutions maintain about consumer financial accounts. For example, while the "right to be forgotten" may make sense with respect to a consumer's social media accounts or other online profiles, it should not be applied with respect to data surrounding a consumer's financial

[3] Colorado and Virginia explicitly chose to provide a complete GLBA exception, while even CA recognized the importance of the exemption for information covered by GLBA.

accounts. It would not make sense to allow customers to "delete" mortgage loan or credit card information.

While it is critical that any new Federal privacy law take into consideration existing privacy laws, such as the GLBA, that apply to financial institutions and avoid provisions that duplicate or are inconsistent with those laws. It should also preempt the existing patchwork of state laws to avoid inconsistent and duplicative requirements that could potentially disrupt financial transactions and the financial system. Having a single federal standard would ensure that consumers receive the same privacy rights and protections regardless of where they may live. A variety of state laws not only makes compliance challenging for financial institutions, but makes it very difficult for consumers to understand – and protect – their own privacy rights; the greater the variation in state laws, the greater confusion and conflict between states and the less transparent the entire regime becomes.

C. **Cyber Attacks, Data Aggregation and Other Threats to Data Security**

Cybersecurity Threats

There are several ongoing trends with the potential to significantly increase risk to the U.S. financial services industry. Cyber-enabled fraud has become a preferred method used by organized crime and is evidenced by the rise in ransomware attacks. FinCEN recently released their financial trend analysis focused on ransomware and stated, "If current trends continue, SARs filed in 2021 are projected to have a higher ransomware-related transaction value than SARs filed in the previous 10 years combined."[4] This rising level of activity, coupled with the difficulty of finding and successfully prosecuting the perpetrators, is certain to result in a continual increase in attacks.

Recently introduced legislative proposals focusing on ransomware and attacks on critical infrastructure center on increased reporting of incidents to various entities such as the

[4] Financial Trend Analysis - Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021, page 3, FinCEN.

Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). While there is value in understanding the scope and scale of attacks, such reporting may not necessarily help any of the victims of these attacks. This is especially true if they create significant and unwelcome burdens, such as trying to meet overly narrow reporting windows while simultaneously trying to manage the impact of an attack. Additionally, some of these proposals do not account for the maturity and reporting requirements already in place in the financial sector. As stated earlier, GLBA has significant reporting requirements already in place for data breaches and the prudential regulators have implemented additional regulations around reporting breaches and cyber-attacks. Legislation focused on reporting cyber-attacks and ransomware should not create redundant reporting requirements for the financial sector. It should also not just focus on reporting but should include strong provisions requiring the federal government and DHS to make effective use of these reports to share threat information with private sector entities in a timely fashion and provide tools that would allow the private sector to respond, mitigate the attacks, and prevent ongoing and future attacks.

Data Aggregation

Data is playing an ever-increasing role in all aspects of our economy, and banking is no different. Today, both banks and fintechs companies offer products that rely on access to a consumer's financial data, which may be housed at another institution. These products range from budgeting tools to income verification for underwriting.

Section 1033 of Dodd Frank guarantees consumers the right to access their financial records in a standardized electronic format. This has been widely interpreted to extend to their ability to share this data with authorized third parties. In 2017 the CFPB began exploring this issue and ultimately issued a set of principles[5] that outline how consumers should be treated when they share their financial data. Since the principles were released, industry collaboration has led to the development of technical standards, industry utilities, and other technologies and practices that can help enable responsible sharing within a safe and secure framework.

[5] See, https://www.consumerfinance.gov/about-us/newsroom/cfpb-outlines-principles-consumer-authorized-financial-data-sharing-and-aggregation/

The CFPB has refocused on this and issued an ANPR in 2021[6]. A recent Executive Order[7] has also highlighted 1033 as a priority. The CFPB currently has 1033 on its rulemaking agenda for Spring 2022. Banks support their customers' ability to access and share their financial data in a secure, transparent manner that gives them control. Consumer financial data is extremely sensitive and must be protected appropriately. As noted above, Congress has recognized the sensitivity of financial information and has provided protections for it under the GLBA, which creates a legal framework for protecting consumer data, and for sharing that data with third parties. However, when data leaves the secure bank ecosystem it is not always afforded these protections.

Traditionally, financial data was shared by a process known as "screen scraping," where a user would forfeit their login credentials creating risks and leaving consumers exposed. Banks, data aggregators, and other technology companies have worked together to invest in more secure API-based standards that give consumers transparency and control when they share their financial data. While we believe that continued industry collaboration is the best way to accomplish our shared goal, there are several regulatory clarifications and other recommendations that would help facilitate the continued development of a responsible data sharing ecosystem.[8]

As the CFPB considers next steps to encourage the development of a data ecosystem that protects consumers, we recommend that the Bureau continue supporting market developments that are already well underway. Overly prescriptive standards risk undermining the progress that has been made and if not well crafted, may leave consumers exposed. It could also stifle innovation that would potentially lead to secure approaches.

In addition, Congress should urge the CFPB to bring data aggregators under direct supervision. By the nature of their business, data aggregators hold a tremendous amount of consumer financial data. It is estimated that data aggregators hold the consumer log-in credentials for tens of millions of customers. Despite this, many consumers don't know that these

[6] See, https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-releases-advance-notice-proposed-rulemaking-consumer-access-financial-records/

[7] See, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/

[8] For a more detailed discussion of ABA's recommendations, see ABA Statement for the Record for the hearing titled "Preserving the Right of Consumers to Access Personal Financial Data" (Sept. 21, 2021) https://www.aba.com/advocacy/policy-analysis/aba-statement-for-the-record-preserving-the-right-of-consumers-to-access-personal-financial-data

intermediaries exist or how much of their information is being collected and shared. Consumers also are likely unaware of the potential risks to their information when it is shared. In most cases consumers do not have a direct relationship with these companies and must trust that their data are being handled appropriately. Proactive supervision is critical to identifying risks before any harm is done to consumers.

A cornerstone of Title X of the Dodd-Frank Act was the authority given to the CFPB to establish a supervisory program for nonbanks to ensure that federal consumer financial law is "enforced consistently, without regard to the status of a person as a depository institution, in order to promote fair competition." Experience demonstrates that consumer protection laws and regulations must be enforced in a fair and comparable way if there is to be any hope that the legal and regulatory obligations are observed. ABA believes that establishing accountability across all providers of comparable financial products and services is a fundamental mission of the CFPB. This is especially important for data aggregators, given the sensitive consumer financial information they store and process.

The bulk of the data processing in this area is managed by a select group of large companies. Accordingly, the CFPB should expeditiously initiate the rulemaking process under Dodd-Frank Act 1024 to define those "larger participants" in the market for consumer financial data that will be subject to regular reporting and examination by the CFPB. Once the CFPB has imposed supervisory authority over the larger data aggregators, it will be better able to monitor – and react to – risks to consumers in this rapidly evolving marketplace.

Congress should also urge the CFPB to coordinate with banking regulators in any rulemaking because implementation of Section 1033 has wide-reaching implications for banks. Because of the sensitive nature of financial data, there are serious safety and soundness concerns that must be addressed. This is why Section 1033 requires the CFPB to "consult with the Federal banking agencies and the Federal Trade Commission," when prescribing any rules.

Third-Party Risk - NCUA Vendor Authority

Congress should take a serious look at the interplay between Credit Union Service Organizations (CUSOs) and the safety-and-soundness risks to the broader credit union system and to the protection of consumer data and privacy. CUSOs are vendors designed to support

credit unions, including in cybersecurity, consumer data protection and other activities. NCUA has no supervisory authority over CUSOs, notwithstanding repeated calls from NCUA Board Members of both political parties as well as the agency's Inspector General.

This regulatory blind spot is more significant now than ever before. In October, over strenuous objections from NCUA's Chairman, the agency finalized a proposal allowing CUSOs to engage in all forms of lending, including auto lending and payday lending. Because of the absence of vendor authority, NCUA has no authority to supervise or examine CUSOs for compliance with federal laws, including data protection, privacy federal consumer financial protection laws, creating what NCUA's Chairman termed a "wild west" of regulation and putting consumers at risk.

It is very troubling that the NCUA has authorized extensive CUSO activities without ensuring that consumers are protected from potential misuse and abuse of those activities. The new CUSO rule will also dilute the common bond requirement, since CUSOs need not serve credit union members, thereby moving credit unions even further adrift from their core mission to their membership. This raises significant competitive and reputation risks for credit unions, and more broadly, for markets and the financial services industry. We encourage the Committee to closely examine this rule and its potential consequences.

D. Access to the Payments System

Today, banks face a range of competitors and disruptors in the financial marketplace, including monoline fintech firms, nonbank payment providers and decentralized finance technologies like cryptocurrency and large technology firms. Only banks, however, offer the full financial services "bundle" of insured deposits that fund consumer and commercial loans, paired with access to the payments system. With this product bundle comes a robust set of data privacy and consumer protections and regulatory supervision. Banks are subject to safety and soundness supervision, regulatory capital and liquidity requirements, consumer protection rules, and affirmative obligations to demonstrate their service to their local areas via the Community Reinvestment Act.

Many nonbank competitors have business models that rely on a kind of regulatory arbitrage in which they can offer one or several aspects of the banking bundle while avoiding the full banking regulatory framework. We see this clearly in the rise of payments charters or

"special purpose national bank charters" that would aim to provide payments system access to companies that—because they do not hold insured deposits or do not lend—would not be subject to the same regulations as banks.

There should be a high bar for access to the payments system. Twenty years ago, in the days after the 9/11 attacks, the country learned just how critical regulated institutions are to payments. At that time, check clearing—managed by the Federal Reserve Banks—involved checks being shipped across the country via overnight airmail delivery. With U.S. airspace closed for several days and checks unable to be processed, the Federal Reserve provided credit on checks on their usual availability schedule. This was only possible because the Federal Reserve supervised the parties participating in the check clearing system and knew they would have sufficient liquidity to cover the checks. Supervision and high standards built up trust, and this lesson should be applied today as the Federal Reserve considers what entities may access our modern digital payments system.

Most importantly, consumers trust banks and the products they provide. According to Morning Consult research commissioned by ABA, nearly half of Americans trust banks more than any other company to keep their data safe, compared to just 12 percent who said the same for nonbank payment providers. Fifty-six percent of Americans say they prefer to receive financial services from a bank versus just 17 percent who said they would prefer to bank with the financial services division of a technology company.[9]

Into the existing payment system, interest has turned to new digital currencies or cryptocurrencies. Cryptocurrencies like bitcoin were designed explicitly to disrupt the banking business model and disintermediate them—allowing for "trustless" finance. Ironically, consumers trust banks *so much* that when they want to access crypto, they would rather do so through their banks. The fintech firm NYDIG surveyed bitcoin holders and found that 81 percent of them would move their bitcoin to a bank if it offered secure storage.[10]

One reason consumers trust banks is that they know their personal data is secure. As noted above, while banks are subject to robust privacy and data security requirements through

[9] See, https://bankingjournal.aba.com/2021/10/morning-consult-poll-banks-get-top-approval-ratings-from-consumers/

[10] See, https://nydig.com/research/nydig-bitcoin-banking-survey

the GLBA and other privacy laws, we understand that some nonbank fintechs take the position that they are not subject to the same requirements. Moreover, some nonbank fintechs may not have the same incentive to protect customer data, and may be more interested in profiting from providing third parties with access to that data. In fact, access to consumer financial transaction data may be the very reason large tech companies are interested in the payments space. We believe that it is important that the CFPB take a more proactive approach in identifying nonbank fintechs that are "financial institutions" for purposes of, and subject to, the GLBA and ensuring that those entities comply with the relevant obligations and limitations imposed by the GLBA. Consumers should receive the same privacy and data security protections at any financial institution.

Congress, the Fed and other policy makers should ensure that the stringent rules for banks should be applied to others looking to offer bank-like services. In that regard, we agree with concerns expressed by CFPB Director Rohit Chopra in his October 28 testimony before the House Financial Services Committee and the Senate Banking Committee about the involvement of big tech companies in the payments system and that they should be subject to the same rules and regulations as local banks and other financial institutions when it comes to data privacy.[11]

Conclusion

Banks of all sizes remain at the center of consumers' and businesses' financial lives and to continue to provide the lifeblood of the U.S. economy. Our members are dedicated to the best possible cybersecurity and to protecting the sensitive data and privacy of consumers. Banks are already subject to a wide-range of data protection, privacy and cybersecurity laws and regulations, and for many years have devoted the time, energy, and resources necessary to secure and protect data and earn the trust of our customers. ABA members are working hard to ensure that consumers remain protected from cyber-attacks, data breaches and other threats that put their sensitive personal and financial data at risk. These threats are constantly evolving and as consumers access a wide range and often novel financial services offerings, it is critical to ensure

[11] See, https://www.consumerfinance.gov/about-us/newsroom/written-testimony-director-rohit-chopra-before-house-committee-financial-services/

they retain the protections they have come to expect from their bank. We support legislation and policy that closes regulatory gaps that put the financial system and consumers at risk.