ICBA
INDEPENDENT COMMUNITY BANKERS of AMERICA®

May 7, 2019

Privacy Rights and Data Collection: The Community Bank Perspective

Chairman Crapo, Ranking Member Brown, members of the Committee, the Independent Community Bankers of America, representing community banks across the nation with more than 52,000 locations, appreciates the opportunity to provide this statement for the record in connection with today's hearing on "Privacy Rights and Data Collection in a Digital Economy." ICBA greatly appreciates your opening the discussion of a critical public policy issue that will only become more significant as the digital economy becomes more pervasive.

Community banks are committed to safeguarding consumer data and honoring consumers' preferences in the use of such data. Attached is a comprehensive statement of community banks' policies, practices, and preferences with regard to the collection and use of personally identifiable information ("PII"), which was previously submitted to this committee in response to your request. Below we highlight the principles which will guide our evaluation of any proposed legislation in this area:

- ICBA supports current privacy standards, such as those in the Gramm-Leach-Bliley Act ("GLBA"). To ensure consumers receive enhanced protection of their personal information, all entities that handle personal information should be required to safeguard this information, in a manner comparable to financial institutions.
- A national breach notification standard would be a good first step to ensure consistent consumer notification in the case of a breach, rather than a patchwork of state laws in this area.
- ICBA supports the current privacy notice requirements. Banks are required, through law and regulation, to provide privacy notices and a myriad of disclosures to consumers and customers about the information they collect and share and the purpose of the information.
- Banks are required to collect certain PII based on various regulatory requirements and provide that information to prudential regulators. Prudential regulators must also appropriately safeguard that information.
- Third parties that contract with banks for services which are not currently subject to examination and supervision should also be examined and supervised for their compliance with the Interagency Guidelines Establishing Standards for Safeguarding Customer Information ("Guidelines"), implementing the Gramm-Leach-Bliley Act.
- The credit reporting agencies ("CRAs"), also known as credit bureaus, should be subject to comparable supervision and examination as banks.
- CRAs should focus on educating and informing the consumer about the use of credit reports and their consumer data collection and sharing practices.
- Non-bank entities accessing customer account data must be held responsible for ensuring the security of the consumer information they are accessing and must be held liable for any data breaches and consumer harm which they cause.
- Consumers must have the same GLBA-like privacy protections with permissioned third parties as they have with banks, including limitations on the use of consumer information and limitations on the disclosure of the consumer's information to third parties.

ICBA looks forward to providing ongoing input on the impact of proposed legislation concerning the collection and use of personally identifiable information ("PII") on community banks and their customers.

ATTACHMENT: March 14, 2019 ICBA Letter to Chairman Crapo and Ranking Member Brown Regarding Community Banks and Consumer Data

ICBA
INDEPENDENT COMMUNITY BANKERS *of* AMERICA®

March 14, 2019

U.S. Senate Committee on Banking, Housing and Urban Affairs
Chairman Mike Crapo
Ranking Member Sherrod Brown
534 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Crapo and Ranking Member Brown:

On behalf of the Independent Community Bankers of America ("ICBA"),[1] thank you for the opportunity to provide our views about potential legislation in the 116th Congress concerning the collection and use of personally identifiable information ("PII"). We welcome the opportunity to discuss our responses in greater detail. The community banking sector takes seriously the ongoing protection of customers' data and privacy and ICBA advocates for constructive policy changes, specifically:

- ICBA supports current privacy standards, such as those in the Gramm-Leach-Bliley Act ("GLBA"). To ensure consumers receive enhanced protection of their personal information, all entities that handle personal information should be required to safeguard this information, in a manner comparable to financial institutions.

[1] The Independent Community Bankers of America® creates and promotes an environment where community banks flourish. With more than 52,000 locations nationwide, community banks constitute 99 percent of all banks, employ more than 760,000 Americans and are the only physical banking presence in one in five U.S. counties. Holding more than $4.9 trillion in assets, $3.9 trillion in deposits, and $3.4 trillion in loans to consumers, small businesses and the agricultural community, community banks channel local deposits into the Main Streets and neighborhoods they serve, spurring job creation, fostering innovation and fueling their customers' dreams in communities

WASHINGTON, DC
1615 L Street NW
Suite 900
Washington, DC 20036

SAUK CENTRE, MN
518 Lincoln Road
PO Box 267
Sauk Centre, MN 56378

866-843-4222
www.icba.org

- A national breach notification standard would be a good first step to ensure consistent consumer notification in the case of a breach, rather than a patchwork of state laws in this area.
- ICBA supports the current privacy notice requirements. Banks are required, through law and regulation, to provide privacy notices and a myriad of disclosures to consumers and customers about the information they collect and share and the purpose of the information.
- Banks are required to collect certain PII based on various regulatory requirements and provide that information to prudential regulators. Prudential regulators must also appropriately safeguard that information.
- Third parties that contract with banks for services which are not currently subject to examination and supervision should also be examined and supervised for their compliance with the Interagency Guidelines Establishing Standards for Safeguarding Customer Information ("Guidelines"), implementing the Gramm-Leach-Bliley Act.[2] • The credit reporting agencies ("CRAs"), also known as credit bureaus, should be subject to comparable supervision and examination as banks.
- CRAs should focus on educating and informing the consumer about the use of credit reports and their consumer data collection and sharing practices.
- Non-bank entities accessing customer account data must be held responsible for ensuring the security of the consumer information they are accessing and must be held liable for any data breaches and consumer harm which they cause.
- Consumers must have the same GLBA-like privacy protections with permissioned third parties as they have with banks, including limitations on the use of consumer information and limitations on the disclosure of the consumer's information to third parties.

Question 1: What could be done through legislation, regulation, or by implementing best practices that would give consumers more control over and enhance the protection of consumer financial data, and ensure that consumers are notified of breaches in a timely and consistent manner?

Community banks and other financial institutions are required by statute and regulation[3] to safeguard personally identifiable information. To ensure consumers receive enhanced protection of their personal information, all entities that handle personal information should be required to safeguard this information, in a manner comparable to financial institutions. With regard to breach notification, a good first step would be to implement a national notification standard, rather than a patchwork of state laws in this area.

Protection of Customer Data

By their very nature, community banks and other financial institutions must collect sensitive nonpublic personally-identifiable information ("PII")[4] about customers to meet their needs for

[2] 12 C.F.R. Part 30, Appendix B. and The Financial Modernization Act of 1999, the "Gramm-Leach-Bliley Act," P.L. 106-102.

[3] The Financial Modernization Act of 1999, the "Gramm-Leach-Bliley Act," P.L. 106-102. The "Interagency Guidelines Establishing Information Security," 12 C.F.R. Part 30, Appendix B. FFIEC IT Examination Handbook, https://ithandbook.ffiec.gov/.

[4] Nonpublic personal information is a term commonly referenced in regulations. Nonpublic personal information is, generally speaking, personally identifiable financial information that is not publicly available. It is also defined as information that is not publicly available and that:

- a consumer provides to a financial institution to obtain a financial product or service from the institution;
- results from the transaction between the consumer and the institution involving service; or a financial product or
- a financial institution otherwise obtains about a consumer in connection with providing a financial product or service.

financial services, which includes an array of deposit and loan services. This information is also used to prevent fraud, identity theft and comply with various regulatory requirements. Safeguarding customer information is central to financial institutions maintaining public trust and retaining customers.

ICBA has consistently advocated that all participants in the payments and financial systems, including merchants, aggregators and other entities with access to customer financial information, should be subject to Gramm-Leach-Bliley Act-like data security standards. Similarly, any entity that processes or holds personally sensitive information about consumers should be required to safeguard that information, just as banks are required. Under current federal law, retailers and other parties that process or store sensitive consumer information are not subject to the same federal data security standards and oversight as financial institutions. Securing personally sensitive data at financial institutions is of limited value if it remains exposed at the point-of-sale and other processing and collecting points. To most effectively secure customer data and thereby protect consumer privacy, all entities that store or process sensitive personal information, and all entities with access to customer financial information, should be subject to and maintain well-recognized standards such those in the Gramm-LeachBliley Act and implementing regulations.

Below is a general overview of some of the legal and regulatory requirements to which banks are subject, and for which they are examined and supervised. These requirements include, but are not limited to, the Gramm-Leach-Bliley Act, the "Interagency Guidelines Establishing Information Security," and the Federal Financial Institutions Examination Council's IT

Examination Handbook. The measures outlined below demonstrate how banks safeguard customer PII. To fully protect citizens, all entities should be required to safeguard PII in a comparable manner.

I. Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act ("GLBA") and its implementing regulations require financial institutions to disclose their information-sharing practices to their customers and to safeguard sensitive data. Additionally, Section 501(b) of the GLBA requires federal banking agencies to establish standards for protecting the security and confidentiality of financial institution customers' non-public personal information.

Subtitle B of GLBA prohibits any person from receiving customer information about another person whether by making a false, fictitious or fraudulent statement to a financial institution representative, to a customer of a financial institution or providing any fraudulent document to a financial institution.[5]

See https://www.fdic.gov/regulations/compliance/manual/8/viii-1.1.pdf and https://www.occ.treas.gov/newsissuances/bulletins/2000/bulletin-2000-21a.html

[5] 15 U.S.C. 6821

II.[2] *Interagency Guidelines Establishing Information Security*

The banking agencies issued their "Interagency Guidelines Establishing Information Security" ("Guidelines")[6] to implement the GLBA requirements. Generally, the Guidelines establish administrative, technical and physical safeguard standards to ensure the security, confidentiality, integrity and proper disposal of customer information.

The Guidelines apply to customer information maintained by, or on behalf of, financial institutions. The Guidelines, among other requirements, mandate that financial institutions implement "a written information security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the bank and nature and scope of its activities."[3]

The Guidelines also specify that the board of directors or an appropriate committee of the board of each insured depository institution shall be involved in approving and overseeing the written information security program.

[2] C.F.R. Part 30, Appendix B.

[3] Federal Register. Vol 66. No. 22. Page 8619.

Each institution is required to assess risk by identifying reasonably foreseeable internal and external threats, and the likelihood and potential damage of those threats. Each institution must also assess the sufficiency of policies, procedures, customer information systems and other arrangements in place to control risks. There are also extensive requirements for managing and controlling the risk which include implementation of a response program.

Finally, it is important to point out that entities contracted by financial institutions are also required to protect customer information in the same manner as the financial institution.[4,5]

III. *Federal Financial Institutions Examination Council ("FFIEC") IT Examination Handbook*[6]

Other legal and regulatory guidance also adequately dictate bank privacy procedures. For example, the Federal Financial Institutions Examination Council's IT Examination Handbook ("FFIEC IT Handbook") is an authoritative document which outlines various guidelines concerning customer data security and privacy that are rightly intertwined within all operational aspects of the bank – from governance to third-party management to information technology.

Breach Notification

ICBA continues to support a single national breach notification standard. Similarly, any legislation related to privacy or data security should also preempt state laws to prevent a continuing patchwork approach to these policy areas.

If a bank becomes aware, upon an investigation, that customer information was improperly accessed, it must notify the affected customers with a description of the incident and what customers may do to protect themselves. This is not true for all entities that store and process sensitive personal information, although it has become a matter of good business practice to notify impacted customers.

Regarding customer notification, ICBA submitted a statement for the record last year for a hearing entitled "Data Security Legislative Solutions: The Community Bank Perspective," which was held before the U.S. House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit on March 7, 2018. Prior to the hearing, then Subcommittee

[4] Board of Governors of the Federal Reserve System. Interagency Guidelines Establishing Information Security Standards "Small Entity Compliance Guide". 2.

[5] To enhance the protection of privacy, ICBA also suggests, in response to Question 3, examination and supervision of all third parties.

[6] See: https://ithandbook.ffiec.gov/

Chairman Blaine Luetkemeyer and Representative Carolyn Maloney circulated a discussion draft of a data security bill, the "Data Acquisition and Technology Accountability Act."[7]

That discussion draft would have created a national data breach notification standard to replace the current patchwork of differing state breach notification laws. In an integrated national economy with a geographically mobile population, consistent standards and expectations are needed to avoid consumer confusion.

Our statement conveyed support for the security requirements in the discussion draft, which would subject other entities to a scalable data security standard. Community banks have long been subject to regulatory mandates that set rigorous data protection practices. These mandates are fundamental and a critical component of the safety and soundness of the overall banking system. With data breaches in the news almost daily, the status quo advocated by other sectors is simply not working for American consumers. Consumers demand that their personal information be held securely and not subject to innumerable breaches. The only way to fulfill this demand is by raising the bar to ensure all entities are subject to comparable standards.

Question 2: What could be done through legislation, regulation, or by implementing best practices to ensure that financial regulators and private financial companies (including thirdparties that share information with financial regulators and private financial companies) provide adequate disclosure to citizens and consumers about the information that is being collected about them and for what purposes?

ICBA supports the current privacy notice requirements. Banks are currently required, through law and regulation, to provide privacy notices and a myriad of disclosures to consumers and customers about the information they collect and share and the purpose of the information.

Disclosure

ICBA supports the current privacy notice requirements. Under current law and regulation, banks must provide privacy disclosures to consumers and customers. Privacy notices must describe whether and how the financial institution shares consumers' nonpublic personal information with other entities.[12] The notices must also briefly describe how financial institutions protect the nonpublic personal information they collect and maintain.[13]

[7] For bill text, see: https://republicans-financialservices.house.gov/uploadedfiles/bills-115-datasa-pih.pdf

An initial notice must be provided when a customer relationship is established.[14] An annual notice must be sent to consumers if the institution has changed its privacy policy since disclosure of its most recently sent privacy policy and if financial institution limits their sharing of customer information.[15] If an institution chooses to disclose nonpublic personal information about a consumer to a nonaffiliated third party, the institution is required to deliver an annual privacy notice.[16] GLBA Section 502 and Regulation P also require that the disclosures provide information for the consumer to opt-out of sharing of personal information with certain nonaffiliated third parties with some exceptions.[17]

[12] 12 CFR 1016.6(a)(1)-(5), (9)

[13] 12 CFR 1016.6(a)(8)

[14] 12 CFR 1016.4(a)(1), 1016.5(a)(1). Financial institutions are also required to provide initial notices to consumers before disclosing any nonpublic personal information to a nonaffiliated third party outside of certain exceptions. [15] A financial institution that does not share nonpublic personal information with nonaffiliated third parties, unless required to do so under certain exceptions, is not required to provide an annual notice. These exceptions include, for example, providing information to third party service providers, securitization, law enforcement and compliance, and consumer reporting; and certain other disclosures described in the GLBA and Regulation P as exceptions to the opt-out requirements. See Bureau of Consumer Financial Protection, 12 CFR 1016, "Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act (Regulation P)" Final Rule. Published 9 August 2018. https://files.consumerfinance.gov/f/documents/bcfp_glba-privacy-notices_final-rule_amendment_201808.pdf.

[16] 12 CFR 1016.4(a)(1), 1016.5(a)(1). Financial institutions are also required to provide initial notices to consumers before disclosing any nonpublic personal information to a nonaffiliated third party outside of certain exceptions.

[17] See Bureau of Consumer Financial Protection, 12 CFR 1016, "Amendment to the Annual Privacy Notice Requirement Under the Gramm-Leach-Bliley Act (Regulation P)" Final Rule. Published 9 August 2018. Page 6. See also 15 U.S.C. 6802(a), (b)(2), and (e); 12 CFR 1016.13, 1016.14, 1016.15.

Information Collection, Regulatory Compliance and Disclosure

In addition to collecting the customer information necessary to provide financial services, financial institutions are required, by statute or regulation, to collect information about consumers and customers in the normal course of doing business to meet regulatory requirements, including obligations to detect and disrupt illicit financial activity. Oftentimes, banks will rely on access to information available from third parties to gather information about customers, particularly in compliance with anti-money laundering "Know Your Customer" rules and Office of Foreign Asset Control obligations. A sampling of these regulatory collection and disclosure laws are detailed below.

I. Bank Secrecy Act

The Bank Secrecy Act and its implementing regulations[18] require the collection and storage of personal information. As part of an effective customer due diligence program a bank must collect and verify the identifying information from each customer before opening the account, including a customer's name, date of birth, address and identification number. At a minimum, a bank must retain this data for a period of five years after an account is closed. The bank must also keep a description of any document that was relied on to verify identity, such as an unexpired driver's license, for five years. Furthermore, a bank should have a thorough understanding of the money laundering or terrorist financing risks of its customer base by collecting information sufficient to develop an understanding of normal and expected activity for its customers. This includes collecting additional data for various transactions, such as wire transfers, the purchase and sale of monetary instruments, and funds transfers.

II. Electronic Fund Transfer Act

The Electronic Fund Transfer Act ("EFTA") requires a disclosure to consumers when using electronic funds transfer ("EFT") that, in the ordinary course of doing business, the financial institution may provide information concerning the consumer's account to third parties (Section 205.7(b)(9)). A financial institution must describe the circumstances under which any information, relating to an account to or from which EFTs are permitted, will be made available to third parties.[19]

III. Right to Financial Privacy Act

On certain occasions, government authorities may request a customer's financial records. The Right to Financial Privacy Act ("RFPA") establishes guidelines that government authorities must follow when requesting a customer's financial records. The RFPA also outlines specific procedures the financial institution must follow upon receiving such a request. This includes,

18 Federal Register. Vol. 81, No. 91. 11 May 2016. https://www.govinfo.gov/content/pkg/FR-2016-05-11/pdf/201610567.pdf. 29398.

19 12 CFR 1005.

among other provisions, providing a customer notice before the financial institution discloses the customer's financial records.[20]

IV. Home Mortgage Disclosure Act

The Home Mortgage Disclosure Act ("HMDA"), implemented by Regulation C, requires many financial institutions to collect, maintain, report, and publicly disclose loan-level information about mortgages. HMDA's original purpose was to provide the public and public officials with data to help determine whether financial institutions are serving the housing needs of the communities in which they are located, and to assist public officials in their determination of the distribution of public sector investments in a manner designed to improve the private investment environment. Congress later expanded HMDA to require financial institutions to report racial characteristics, gender, and income information on applicants and borrowers. On an annual basis, HMDA requires that its loan/application register ("LAR") data be submitted and that the institution retain a copy of its LAR for at least three years.

V. The Dodd-Frank Wall Street Reform and Consumer Protection Act

Section 1100F of The Dodd Frank Wall Street Reform and Consumer Protection Act (the "Dodd Frank Act") requires a disclosure to the consumer if a credit score was used in taking adverse action on a credit application. Section 615(a) of the Fair Credit Reporting Act ("FCRA"), as amended by the Dodd-Frank Act, requires a person to provide an adverse action notice when the person takes an adverse action based in whole or in part on information in a consumer report. The FCRA's requirements for adverse action notices apply only to consumer transactions and are designed to alert consumers that negative information was the basis for the adverse action. A creditor that obtains a credit score and takes adverse action is required to disclose that score, unless the credit score played no role in the adverse action determination. Adverse action notices typically adopt the format of the model form provided by the Consumer Financial Protection Bureau ("CFPB") and should disclose that adverse actions were taken based on information provided from a consumer reporting agency and that the consumer has the right to dispute the accuracy or completeness of any information in a consumer report, among other provisions.

[20] 12 U.S.C. 3401, *et seq.*

Question 3: What could be done through legislation, regulation, or by implementing best practices to give citizens and consumers control over how financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) use consumer data?

Banks are required to collect certain PII based on various regulatory requirements and provide that information to prudential regulators. Prudential regulators must also appropriately safeguard that information. Additionally, as an added consumer protection, third parties that contract with banks for services which are not currently subject to examination and supervision should also be examined and supervised for their compliance with the Interagency Guidelines Establishing Standards for Safeguarding Custom Information ("Guidelines"), implementing GLBA.

Prudential regulators must also appropriately safeguard consumer information

As illustrated in the previous answer, there are numerous regulatory requirements by which banks must collect PII and then share that information with financial regulators. It is critical that the prudential regulators maintain the confidentiality of the information provided to them.

No company, financial institution, or government agency is exempt from insider threats or criminals breaking into their systems and yanking the personal information of their customers, employees, and/or general stakeholders. In fact, the prudential banking regulators have had their share of data security incidents. For example, in November 2015, a former employee at the Office of the Comptroller of the Currency removed more than 10,000 records by downloading files onto thumb drives without receiving prior authorization.[8] In 2018, the Federal Deposit Insurance Corporation's Office of Inspector General released a "Special Inquiry Report," which detailed several data incidents and a data breaches, one in which an employee placed data on personal storage devices.[9] The Federal Reserve appears to have been under constant attack by would-be hackers according to news reports in mid-2016; whether hackers have been successful in accessing sensitive records remains to be seen.[10] In 2014, a National Credit Union Administration examiner lost a flash drive containing personal information for members of a credit union in Palm Springs, California.[24] Additionally, the CFPB paused the collection of personally sensitive data from companies until an independent review found that "externally facing bureau systems appear to be well-secured."[11]

---

[8] OCC. "OCC Notifies Congress of Incident Involving Unauthorized Removal of Information." 28 October 2016. https://www.occ.gov/news-issuances/news-releases/2016/nr-occ-2016-138.html

[9] FDIC, Office of Inspector General. "Special Inquiry Report: The FDIC's Response, Reporting and Interaction with Congress Concerning Information Security Incidents and Breaches. April 2018. OIG 18-001. https://www.fdicoig.gov/sites/default/files/report-release/OIG-18-001.pdf

[10] Reuters. "Exclusive: Fed Records Show Dozens of Cybersecurity Breaches." 2016. June 1. https://www.reuters.com/article/us-usa-fed-cyber-idUSKCN0YN4AM [24] Credit Union Times. "NCUA Examiner Blamed for Data Breach. 15 December 2014.

https://www.cutimes.com/2014/12/15/ncua-examiner-blamed-for-data-breach/

[11] Wall Street Journal. "CFPB to Resume Private Consumer Data Collection. 31 May 2018. https://www.wsj.com/articles/cfpb-to-resume-private-consumer-data-collection-1527796179

ICBA is troubled that liability from a potential breach into any of the prudential regulators' systems could be unfairly assigned to community banks that securely submitted their data. Too often, the breached entity skates by while financial institutions are left to mitigate damages to their customers. For example, when Home Depot was breached in 2014, community banks were responsible for replacing payment cards, notifying customers, implementing enhanced monitoring, and reimbursing customers for fraudulent transactions. In the recent Equifax breach, sensitive personal information was accessed by a yet-unknown source. Community banks will face untold damages due to the unique circumstances of this massive data breach. Because of the Equifax breach, community banks must institute additional protective measures to deter customer identity theft and fraudulent transactions. Community banks will also bear the responsibility for costs associated with payment card cancellation and replacement, fraudulent charges, customer notification, closing affected accounts, and lost interchange fees; all while monitoring the risk of continuing to exchange information with Equifax. A breach into the prudential regulators' systems could have strikingly similar effects on the nation's community banks, particularly when considered in context of the data incidents described above.

Third Party Examination and Supervision

The protection of personal information is critical to protecting customer privacy. Banks contract with third parties for a variety of reasons, some of which include adding efficiency to back office operations. At times, it becomes necessary to share sensitive personal information with third parties. According to the FFIEC IT Handbook, banks that have contractual relationships with third parties and share personal information with these third parties are required to oversee service provider arrangements by (1) exercising appropriate due diligence in selecting service providers; (2) requiring service providers by contract to implement appropriate measures designed to ensure the security and confidentiality of the institution's "customer information"; and (3) where indicated by the institution's risk assessment, monitoring service providers to confirm that the service providers have satisfied their contractual obligations, including by reviewing audits, summaries of test results, or other equivalent evaluations of service providers.[26]

As an added protection for consumers, examinations of all third parties would ensure that third parties are safeguarding consumer data in compliance with GLBA and will ultimately better protect the consumer.

[26] See the FFIEC IT Examination Handbook on Information Security, Sections II and III.D. Also see the

Outsourcing Technology Services Booklet – "Before entering into outsourcing contracts, and throughout the life of the relationship, institutions should ensure the service provider's physical and data security standards meet or exceed standards required by the institution. Institutions should also implement adequate protections to ensure service providers and vendors are only given access to the information and systems that they need to perform their function. Management should restrict their access to financial institution systems, and appropriate access controls and monitoring should be in place between service provider's systems and the institution."

Question 4: What could be done through legislation, regulation, or by implementing best practices by credit bureaus to protect consumer data and to make sure that information contained in a credit file is accurate?

ICBA recommends that the credit reporting agencies ("CRAs"), also known as credit bureaus, be subject to comparable supervision and examination as banks. Additionally, CRAs should focus on educating and informing the consumer about the use of credit reports and their consumer data collection and sharing practices.

Protecting Consumer Data

Protecting consumer data is a critical component to maintaining the financial services ecosystem. Banks are held to a high standard as explained in the previous responses. However, CRAs are not subject to the same supervision and examination as banks, despite the vast amount of PII they process, maintain and store. For example, the credit bureaus must comply with rules set by the Federal Trade Commission and CFPB with regard to selling consumer data, but they are not subject to the same examination and supervision as banks.

Last Congress, Representative Patrick McHenry introduced H.R. 4028, which, among other things, would subject CRAs to examination and supervision by a banking regulator to be determined by the FFIEC. ICBA strongly supported, and continues to support, this approach.

The massive data breach at Equifax, which exposed the personal data of 148 million American consumers, shows the ongoing vulnerability of CRAs. While CRAs are subject to the data security standards of the Gramm-Leach-Bliley Act (GLBA), they are not examined or supervised for their compliance with these standards in the same manner as financial institutions, yet they hold equally critical, personally sensitive information about consumers. This is a grave weakness and disparity in our current system.

Data Accuracy

Accurate information within a credit file is critical for end-users of credit reports. These reports are used to make important decisions about a customer's ability to obtain and responsibly use credit. CRAs should educate and inform consumers about the use of credit reports and their

information collection and sharing practices. Education should stress to the consumer the importance of ensuring their reports contain accurate, complete and verifiable information, and the steps taken to secure data.

Question 5: What could be done through legislation, regulation, or by implementing best practices so a consumer can easily identify and exercise control of data that is being (a) collected and shared by data brokers and other firms and (b) used as a factor in establishing a consumer's eligibility for credit, insurance, employment, or other purposes.

Non-bank entities accessing customer account data must be held responsible for ensuring the safety and security of the consumer information they are accessing and must be held liable for any data breaches and consumer harm which they cause. **At a minimum, consumers must have the same GLBA-like privacy protections with permissioned third parties as they have with banks, including limitations on the use of consumer information and limitations on the disclosure of the consumer's information to third parties.**

While ICBA fully supports consumers' rights to have access to their own information, such access should be properly balanced with ensuring that consumer privacy is not needlessly threatened. Protecting the privacy of consumer information is at the heart of the community bank business model. Community banks are strong guardians of the security and confidentiality of customer information as a matter of good business practice.

Information that is gathered by entities outside of the financial services industry is not held to the same standard as it relates to safeguarding information. Once information is shared with permissioned third-parties, consumers may no longer have control of their personal and financial information. The potential for abuse is real and can be extremely harmful to consumers. This leaves consumers vulnerable to entities that may mislead them about who they are or what they do with the information they collect and places an extraordinary burden on consumers to be vigilant in their research and knowledge of firms to which they may provide their online account credentials. For this reason, ICBA has profound concerns that non-bank entities which may be authorized by consumers to access their information and store their bank login credentials do not take the same care in protecting consumer privacy and data as community banks. It is also worrisome that many third parties which seek to access customer data are not well capitalized and may have no real assets. In fact, these firms may be no more than one person developing an app on his or her laptop. When there is a loss, they may be financially unable to make the consumer whole.

While financial institutions are prohibited from sharing account numbers or similar access codes for marketing purposes, and from sharing personal information with nonaffiliated third parties without giving customers an "opt-out notice" that describes customer's rights to information being shared, other non-financial entities are not subject to the same rules. Selling consumer data for marketing purposes is an appealing revenue source which could be utilized by some unscrupulous businesses.

At a minimum, consumers must have the same GLBA-like privacy protections with permissioned third parties as they have with banks, including limitations on the use of consumer information and limitations on the disclosure of the consumer's information to third parties.

To further privacy protections, there is opportunity to set limits and safeguards on which data is available to data aggregators, data brokers and other third-parties. Granting carte blanche access to these entities increases the potential for unauthorized use and inadvertent breaches. In addition to setting limits on the type of data collected, Congress has an opportunity to limit how thirdparties and data aggregators use the data. These limitations should reflect the reasonable expectations of consumers or explicit consumer instructions on the use of such data.

Data aggregators and other third-parties should also provide transparency on data access. If data aggregators and third-parties seek permission from consumers to access a their data, then consumers should be provided with clear disclosures on which data is being collected and how it will be used, along with any downstream usage of that data, (i.e., if and whether it will be soldoff to any subsequent third-parties).

Finally, to ensure that any legislation, regulation, or best practices is implemented by data aggregators and other third-parties, the CFPB should have formal and explicit supervision and enforcement authority over these entities.

While data aggregators and other third-parties are focused on accessing and utilizing consumer data, there must be a serious recognition that not all data is equal. Financial data is unlike all other forms of data, and as such, must be accessed and used with the utmost caution. As Congress continues to examine and explore this area, it is incumbent for legislation, regulation, or best practices to address these issues.

Community Banks Should Not Have to Bear the Cost and Risk of Ensuring Safe Third-Party Access

As community-based institutions, a community bank's success is in large part dependent on its reputation. Maintaining the integrity of customer accounts is of utmost importance to community banks, not only because it is required by law, but also because it is the right thing to do. If a customer experiences an adverse event which results in financial loss caused by a breach or failure by a permissioned third party, it is likely that customer will look to his or her bank with the expectation of being made whole. When a loss occurs through no fault of a community bank, but because of the failing of a third party, that third party should be held responsible. For example, there should be certainty as to whether consumers would be protected under the Electronic Fund Transfer Act for unauthorized debits when consumers share their account information.

Furthermore, community banks have a vital stake in containing any damage caused by hackers, identity thieves and breaches to third parties. Regardless of where a breach occurs, banks are the stewards of the customer financial relationship. They take measures to restore consumer confidence in the financial system and absorb any upfront costs, which may be significant, of third-party intrusions by responding to customer concerns and inquiries, protecting against fraud and absorbing other expenses. Therefore, any costs associated with a breach or hack should be borne by the entity that incurs the breach. Firms with third-party access to a consumer's account should bear full liability for any consumer harm resulting from a breach to its system.

ICBA appreciates the opportunity to provide our views on these questions. We welcome a further discussion with the Committee on these and other related topics. Should you have any questions, please reach out to Jeremy Dalpiaz of my staff by email at Jeremy.Dalpiaz@icba.org or by phone, 800-422-8439.

Sincerely,

Rebeca Romero Rainey
President and CEO