http://www.regulations.gov.

February 21, 2017

Ms. Monica Jackson
Office of the Executive Secretary
Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552

Re: Docket No. CFPB-2016-0048, Request for Information Regarding Consumer Access to Financial Records

Dear Ms. Jackson

The Independent Community Bankers of America[1] appreciates the opportunity to provide comments to the Consumer Financial Protection Bureau (CFPB or Bureau) on its Request for Information (RFI) Regarding Consumer Access to Financial Records. Through this RFI, the CFPB is seeking to better understand the consumer benefits and risks associated with market developments that rely on access to consumer financial account and account-related information.

[1] The Independent Community Bankers of America, the nation's voice for nearly 6,000 community banks of all sizes and charter types, is dedicated exclusively to representing the interests of the community banking industry and its membership through effective advocacy, best-in-class education and high-quality products and services.

With 51,000 locations nationwide, community banks employ 700,000 Americans, hold $4.0 trillion in assets, $3.2 trillion in deposits and $2.7 trillion in loans to consumers, small businesses and the agricultural community. For more information, visit ICBA's website at www.icba.org.

I. Summary of ICBA's Position

While ICBA supports responsible financial services innovation, we urge the CFPB to carefully consider the privacy, regulatory burden, data security, and legal implications posed by third-party account access. Some financial web services may offer benefits to consumers; however, when third parties are allowed to access customer accounts there are tradeoffs that must be considered.

ICBA has profound concerns that non-bank entities which access customer information and store bank login credentials do not take the same care in protecting consumer privacy and data that community banks do. It is also worrisome that many third parties which are seeking 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. ICBA strongly encourages the Bureau to consider these risks when reviewing the responses to this RFI.

The integrity of consumers' data and privacy is only as strong as the weakest link protecting that information, and as more parties handle a consumer's data, the risk of breach and/or loss only increases. Furthermore, to ensure a level playing field, non-bank entities accessing customer account data must be held responsible for ensuring the safety of the consumer information they are accessing and must be held liable for any data breaches and consumer harm which they cause. Finally, ICBA believes that while Dodd-Frank is clear that financial institutions must allow consumers access to their financial records, there is no statutory provision that these same rights should be carried over to third parties which consumers have granted their online access credentials (permissioned third parties).

II. Background

ICBA believes that many, if not nearly all, community banks that maintain online customer account access are already providing data to permissioned third parties. Community bank online platforms vary widely in the capabilities they offer consumers and, by extension, permissioned third parties. Many community banks are heavily reliant on their core processors and other vendors for developing and maintaining online account access. Consequently, the capabilities of a community bank's online presence will in large part be dictated by the type of support its vendors provide. Technical issues and legacy systems may also limit the type of data and the method by which it can be delivered to

permissioned third parties. Additional capabilities will almost always lead to increased costs which many community banks with smaller customer bases will find harder to absorb.

Community banks are experiencing a rapidly evolving marketplace, with new permissioned third parties seeking to access their networks on a regular basis. Community banks report that it is virtually impossible to control how or to whom consumers provide their online access credentials. While community banks closely monitor their online systems, the sheer number of permissioned third parties and volume of requests often makes it impractical to conduct any thorough vetting of legitimate requests to access customer information. Furthermore, many entities seeking account access make little information about themselves publicly available, thereby compounding the difficulty community banks experience in vetting permissioned third parties.

Some community banks also make data aggregation services available to their customers for a variety of products, including inter-bank payments, automated advisors, and dashboards. Offering these services enables community banks to deepen the customer relationship, minimize payments risk, and remain competitive in a dynamic marketplace. These tools are often developed by vendors. Anecdotal feedback from ICBA members indicates that some community banks are aggressively exploring and offering data aggregation or financial dashboard services. Community banks that offer these services report varying levels of customer use.

III. Threats to Consumer Privacy

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.

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. The relationship between community banks and their customers is built on trust and a long-standing commitment to protect customer privacy. Firms which seek to provide services which require consumers to provide their online account credentials may not have the same commitment to protecting consumer privacy and could use or resell the financial data for cross-selling and other targeted marketing purposes, without the explicit consent of the consumer.

Community banks are highly regulated and have been subject to rigorous security requirements for decades. Regulators require the banking sector to protect not only their own systems but their customer data as well. Additionally, they must have policies and procedures in place to identify, prevent, and mitigate identity theft. As a result of the Gramm-Leach-Bliley Financial Modernization Act of 1999 (GLBA), banks are required to have administrative, technical, and physical safeguards and standards in place to ensure the security and confidentiality of customer information. However, protecting consumers' account data at banks is of limited value if it remains underprotected or exposed by other users.

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.

However, with the promise of convenience and ease in financial management, debt monitoring, budgeting, and savings growth, some consumers provide firms with confidential and personal information with little thought to the dangers of sharing such sensitive data. Some consumers will easily provide their online account credentials, user names, passwords, answers to knowledge-based security questions, and other forms of authentication, making their private information susceptible to broad dissemination and identity theft. This places on the third party an obligation to store and protect a customer's online credentials. If this information is breached, a fraudster could have access to a consumer's entire financial history.

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.

IV. Data Security Risks

Community banks and the financial services industry continue to vigorously defend against security threats and take their role in securing customer data and personal information very seriously. Beyond existing regulatory and statutory requirements, safeguarding customer information is central to maintaining public trust and key to long-term customer retention. As such, community banks take a variety of steps to protect the integrity of their customers' accounts, including monitoring for indications of suspicious activity and reimbursing customers for confirmed fraudulent transactions.

However, not all entities or industries place such importance on protecting their customer data. As we have seen time and time again, bad actors look for ways to obtain consumers' personal information. Fraudsters and hackers continuously look for ways to take over financial accounts, steal identities to open new accounts, and divert government benefits, tax returns, or balances for their own use. The financial account data and sensitive personal information collected, transmitted and stored by firms unrelated to a community bank, coupled with various technological solutions make account aggregators attractive targets for hackers. These threats are continuously evolving. And while banks have a long history of understanding and continually adapting their technologies and connections to mitigate new threats, the same cannot be said for unregulated or under-regulated entities which do not face bank-like supervision and enforcement.

That is why data security must be a shared responsibility. Securing consumer data must be a core responsibility in all industries – not just the financial sector. Particularly as new market entrants are offering products and services using consumer-permissioned, electronically sourced bank account data. While community banks and the financial services sector go to great lengths to protect consumer data, all entities that store or have access to consumer account data must be held to the same security standards as banks.

Unfortunately, once information is shared with entities outside of a customer's "home" financial institution, the existing privacy protections are limited and the security mechanisms currently in place will only be as strong as the weakest link. Weak security standards in non-regulated businesses make the consumer vulnerable to unscrupulous fraudsters and identity thieves.

V. Burdens Third-Party Access Imposes on Community Banks

ICBA is concerned that the CFPB may in the future develop rules that dictate how community banks share customer information with permissioned third parties. Requiring that community banks provide unfettered access to permissioned third parties would impose tremendous burdens, as well as financial and reputational risks. When a customer discovers fraud, they usually contact their bank first, rather than a third party.

Community banks continue to work through implementing and complying with an unprecedented number of new and amended regulatory requirements put into effect over the past several years. These new rules have touched virtually every consumer product and service community banks offer. New rules have created additional procedures and paperwork for all banks, but community banks have a harder time absorbing the costs imposed by these requirements because they do not have the resources or customer base of larger firms. These regulatory burdens continue to drive community bank consolidation with a corresponding reduction in consumer choice.

ICBA is also concerned that regulations in this area could stifle security and authentication innovation in protecting consumer's information by not properly allowing for evolution in data security and information sharing in the coming years. As accessing online accounts moves past the familiar username and account password model, new rules or requirements may be stuck in the old paradigm thereby introducing weaknesses in future security advances

VI. 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.

Unfortunately, many third parties which are seeking 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. ICBA strongly encourages the Bureau to consider these risks when reviewing the responses to this RFI.

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 any 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.

VII. There is No Legal Basis to Require Banks to Provide Permissioned Third Party Access

The Bureau has issued this RFI citing its authority under Section 1033 of the Dodd-Frank Act which provides for consumer rights to access information. More specifically, section 1033 requires that "[s]ubject to rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, information in the control or possession of such person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, or series of transactions, to the account including costs, charges, and usage data."[2]

The entire text of Section 1033 concerns consumer access, in no place is there any language which indicates that Congress intended the Bureau to ensure permissioned third parties can access customer account data. Consumers of course must be free to use their own account data as they see fit. Consumers can download their data and upload it if they so wish. However, the CFPB simply does not have authority to require community banks to open their systems to third parties, and other entities which may have not implemented appropriate security processes or procedures.

VIII. Conclusion

ICBA asks the CFPB to carefully consider these comments and address our concerns that the Bureau may be developing rules which would dictate how

[2] 12 U.S.C. 5533(a).

community banks provide permissioned third parties account access. Community banks must be able to protect customer data without having to meet new regulatory mandates which increase the risk of breach and/or consumer loss. Please contact me, Joe Gormley, at Joseph.Gormley@icba.org or (202) 659-8111 with any questions regarding our comments. We look forward to working with the Bureau on this important issue.

Sincerely,

/s/

Joseph M. Gormley
Assistant Vice President and Regulatory Counsel