American Bankers Association
Building Success. Together.

Robert A. Morgan
Vice President
Emerging Technologies
202-663-5387
rmorgan@aba.com

February 21, 2017

By electronic submission to: FederalRegisterComments@cfpb.gov

Consumer Financial Protection Bureau
1275 First St. NE
Washington, D.C. 20002

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

Ladies and Gentlemen:

The American Bankers Association (ABA)[1] welcomes the opportunity to comment on the Consumer Financial Protection Bureau (Bureau)'s Request for Information Regarding Consumer Access to Financial Records (RFI)[2]. The Bureau is seeking comment to better understand the consumer benefits and risks associated with market developments that rely on access to consumer financial account and account-related information.

Technology has facilitated the creation of an unprecedented amount of consumer financial data. The inherent sensitivity of this data highlights the timeliness of this RFI and the need to ensure that financial data are handled appropriately. ABA fully supports the customer's ability to access and share their financial data in a secure, transparent manner that gives them control. This letter will identify regulatory gaps that must be filled and suggest steps to facilitate access to financial data that protects and empowers consumers.

Background and Summary of Comment

Technology is changing fundamentally how financial services are delivered. Customers are adopting new technologies and are relying increasingly on these new technologies to interact with their financial institutions. Mobile access and digitization of traditional services have brought an explosion in the amount of financial data being created.

The unprecedented proliferation and availability of this data has led to the development of new financial technologies (fintech). ABA believes that innovation in financial services continues to have tremendous potential to benefit customers as it has throughout the history of banking. Innovation can give customers improved knowledge about and control over financial products they use every day, expand credit access to more borrowers, and promote financial inclusion.

---

[1] The American Bankers Association is the voice of the nation's $16 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard $12 trillion in deposits and extend more than $9 trillion in loans.

[2] Request for Information Regarding Consumer Access to Financial Records, 81 Fed. Reg. 83806 (Nov. 22, 2016). Available at http://files.consumerfinance.gov/f/documents/112016_cfpb_Request_for_Information_Regarding_Consumer_Access_to_Financial_Records.pdf

Banks are innovating and partnering with technology companies to deliver these benefits to their customers. As banks innovate, they do so within an established regulatory framework, backed by intense supervision and oversight, that ensures robust customer protection.

In addition, financial innovation is happening outside of the banking system. Technology focused startups are building products that rely on access to consumer financial data. As a result, the demand for consumer financial data has increased dramatically, creating opportunity for companies that broker these data. Banks fully support consumer access to data and are working to ensure that their customers can share their financial data safely.

However, sharing financial information is not the same as sharing information about where a consumer ate dinner. Consumer financial data are extremely sensitive and must be protected appropriately. Accordingly, Congress has recognized the sensitivity of financial information and has provided protections for it in the Gramm-Leach Bliley Act of 1999 (GLBA) – ***obligations that apply to all parties that hold it throughout its lifecycle***.

Banks take very seriously their responsibilities to their customers to maintain the highest level of privacy, security, and control over their financial assets and transactions. It is why this issue of data sharing – and getting it right – is so important to our industry. Today, consumers trust that their financial data are being protected and handled appropriately. This trust is critical to the functioning of the financial system, and is the reason banks dedicate tremendous resources to safeguarding financial data.

Current practices in the data aggregation market, however, may leave consumers exposed and create risk that undermine this trust. Consumers today are offered a Faustian bargain in which their desire for technology-driven convenience is exchanged – often unknowingly – for increased potential of catastrophe, by handing over the keys to their financial vault. When consumers share their login credentials with an aggregator, they are giving the aggregator *carte blanche* access to their financial data, including information about things such as their life savings or retirement account. Yet consumers are not given adequate information or control over what information is being taken, how long it is accessible, and how it will be used in the future.

Moreover, consumers are unaware of the differences in the legal and supervisory standards applicable to bank and nonbank participants in the financial services marketplace. Once the information is shared, it leaves a secure bank environment, where it is accorded longstanding legal protections, and it is released into the data services market where it is accorded no more special status than data created through a consumer's use of a social media platform.

There is a better way forward. We can empower consumers to share their financial data, without assuming the risk they take on unknowingly today. We believe three core principles should set the framework for how data are shared and how consumer data are treated:

- **Security:** Consumers deserve bank-level security and protection regardless of where they choose to share their data. This means that consumer data are treated the same – and subject to GLBA protections – whether at a bank or a third party.

- **Transparency:** Consumers must have transparency about how companies use their financial data. It should be clear to consumers what data a fintech company are accessing, how long the company is holding this data, and how it is using the data.

- **Control:** Consumers should have control over the access and use of their data. Customers should have control over what information is shared and how it is used. Intuitive control would allow consumers to see easily who is authorized to receive their data, modify what access they have, and revoke that access when a service is no longer used. If consumers can easily control the data being accessed, they can better understand what is being used and protect themselves accordingly.

More specifically, ABA offers the following recommendations to ensure that consumers can continue to benefit from innovative products and services within a resilient financial services market that protects and advances privacy and data security. While larger institutions have the resources to develop secure portals and the ability to impose privacy and data security requirements through contractual provisions negotiated with aggregators, community banks typically lack the resources to negotiate directly with aggregators. We believe these regulatory clarifications and actions are necessary to ensure that customers of all banks – regardless of their asset size – can benefit from financial innovation. Accordingly, ***ABA recommends that the Bureau use existing regulatory authorities to close regulatory gaps and ensure that consumer financial data are accorded baseline privacy and security protections regardless of where the data reside.***

We recommend the Bureau:

- Clarify that data aggregators are "financial institutions" subject to the requirements of the Gramm-Leach-Bliley Act (GLBA) that apply to financial institutions under the FTC's Safeguards Rule and Bureau's Regulation P.

- Take steps to ensure data aggregators are subject to the same standards as depository institutions for safeguarding financial data and notifying customers about security breaches.

- Clarify that data aggregators are "service providers" under the Electronic Funds Transfer Act (EFTA) and are liable for unauthorized electronic fund transfers that exceed the consumer's liability under EFTA.

- Identify "larger participants" in the market for consumer financial data that are subject to supervision by the Bureau and begin to supervise those entities.

ABA believes that innovations in financial services can provide consumers with tremendous value. By fairly addressing both the opportunities and risks, we have the ability to give consumers innovative services that they can trust. We believe the specific steps outlined above provide the base upon which to build to provide the security, transparency and control for consumers so they can unlock the true potential of fintech and take charge of their financial future.

I. Data Access is Only Part of a Much Larger Story

The Bureau seeks to enable consumers to access and share their financial records so that they can realize the benefits technology promises, and in particular, so consumers have better understanding of their finances. While access is the focus of the RFI,[3] it is only part of a much larger story. Access cannot be divorced from security, transparency, and control. ABA believes that consumers only benefit from access when the financial data retains existing legal protections, regardless of the entity that holds it, and consumer trust in the financial system is maintained. As such, we believe that any conversation about sharing financial data must include full consideration of the rights and protections given to consumers in regard to their financial data.

Traditionally, consumer financial data have been held only at regulated financial institutions and third party service providers that directly contract with them, which are subject to GLBA. This regulatory framework along with effective supervision ensures that customers' sensitive financial data receive all legal protections. The emergence of the financial data services market has challenged this model. Today consumers' financial information can be pulled out of a secure bank system by a data aggregator and passed along to the aggregator's customers.

Yet few consumers appreciate the risks presented when they provide access to financial account data to non-bank fintech companies. In fact, they may believe mistakenly that the information is afforded the same protections as those that apply when depository institutions handle the data.

Given the structural change that has taken place and to ensure that current practices in the consumer financial data market do not undermine longstanding consumer trust in financial service providers, we urge the Bureau to take a holistic approach to data-sharing that addresses access while also ensuring that consumer data are appropriately protected throughout their lifecycle.

II. Financial Data is Sensitive and Accorded Special Status Under Law

U.S. law has long accorded special status to consumer financial information given the sensitivity of the information. To ensure consumer financial information is properly secured, it is subject to laws related to privacy, data protection, and restrictions on data use and accessibility. For example, GLBA imposes on financial institutions obligations to respect customer privacy and to safeguard financial information. Specifically, §501 of that law imposes on financial institutions 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."[4]

GLBA's privacy provisions, with certain exceptions, prohibit financial institutions from disclosing nonpublic personal information about a customer to nonaffiliated third parties unless

---

[3] In the summary of the RFI, the CFPB noted that its purpose for issuing the RFI was that §1033 of the Dodd-Frank Act "provides for consumer rights to access financial account and account-related data in usable electronic forms."

[4] 15 U.S.C. § 6801(a)

the institution complies with various notice and opt-out requirements. These provisions also require that customers receive notices that clearly describe the financial institution's policies and practices to protect the confidentiality and security of that information. According to GLBA's implementing regulations, these privacy notices must be "clear and conspicuous;" in other words, they must be understandable and designed to call attention to the nature and significance of the information contained in the notice.

GLBA also requires financial institutions develop, implement, and maintain a comprehensive information security program to: (1) ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Under GLBA Title V, Subtitle B, both the FTC and the prudential banking agencies have adopted regulations that require steps to safeguard customer data. The FTC Safeguards Rule[5] (which applies to nonbanks) only sets out the standards and stops short of the important requirements adopted by the federal banking agencies[6] for institutions to notify customers as quickly as appropriate after a breach to allow customers to take steps to protect themselves in the event their information may have been compromised. At a minimum, banks must assess the nature and scope of the incident and the information systems and customer data that may have been accessed. Banks must also take appropriate steps to control the incident and prevent further unauthorized access and to notify customers and the appropriate authorities.

Finally, banks supervised by the banking agencies are subject to regular examination of their information security practices; those found not in compliance with GLBA privacy and safeguards rules must become compliant or incur monetary penalties and public cease and desist orders.[7] This regular oversight ensures that appropriate resources are allocated to protect consumer financial data.

What is important to recognize, is the fact that the provisions of GLBA underscore Congressional recognition of the critical importance of protecting financial data.

---

[5] 16 C.F.R. 314

[6] As stated in the *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* issued March 23, 2005, "The interpretive guidance states that financial institutions should develop and implement a response program designed to address incidents of unauthorized access to sensitive customer information maintained by the financial institution or its service provider." *See* BD. OF GOVERNORS OF THE FED. RESERVE SYS., FEDERAL BANK AND THRIFT REGULATORY AGENCIES JOINTLY ISSUE INTERAGENCY GUIDANCE ON RESPONSE PROGRAMS FOR SECURITY BREACHES (2005) available at https://www.federalreserve.gov/boarddocs/press/bcreg/2005/20050323/. *See also*, e.g., FED. DEPOSIT INS. CORP., FDIC FIL-27-2005, GUIDANCE ON RESPONSE PROGRAMS FOR UNAUTHORIZED ACCESS TO CUSTOMER INFORMATION AND CUSTOMER NOTICE (Apr. 1, 2005) available at https://www.fdic.gov/news/news/financial/2005/fil2705.pdf.

[7] Further illustration of the special status of financial information is the Fair Credit Reporting Act (FCRA), which limits accessibility and use of consumer reports such as credit reports. Under FCRA, only those with a "permissible purpose" are permitted to access information contained in consumer reports. For example, entities may obtain credit reports only if the consumer has requested credit, has an existing credit account, or if the report is needed in connection with a business transaction the consumer has initiated.

III. Financial Data Should Be Consistently Protected Regardless of Where the Data Originated, Where They Are Transferred, and the Type of Company Using or Storing Them

Consumers should expect their financial data to be protected whether held by a bank or a data aggregator. As discussed above, GLBA provides a robust framework to protect "nonpublic personal information" of a consumer that is held by a "financial institution." ABA believes that data aggregators fall under the GLBA's definition of "financial institution" and therefore should be subject to all the rules that apply to all other financial institutions. This ensures that data protections apply consistently regardless of where the data originated, where they are transferred, and what type of company is using or storing the data.

Congress used an intentionally robust and expansive definition of "financial institution" in GLBA, which encompasses "any institution the business of which is engaging in financial activities as described in [the Bank Holding Company Act of 1956, §4(k).]"[8] This definition includes not only banks, but as interpreted by the Board of Governors of the Federal Reserve, also encompasses any entity that provides data processing, data storage and data transmission services for financial data.[9] In other words, GLBA clearly applies to data aggregators.

Despite the importance of protecting this sensitive information, it is not clear whether data aggregators comply with the law. Even with the clear congressional intent and broad definition, it is apparent that many aggregators have put their interests above consumers and chosen to ignore or avoid implementing protections as if GLBA does not apply to them. ***Therefore, is critical that the Bureau articulate clearly that data aggregators fall within GLBA's definition of "financial institution"*** subject to the requirements of GLBA as they apply to other financial institutions. This would ensure that consumers receive the GLBA security protections as implemented by the Bureau's Regulation P and the FTC's Safeguards Rule.[10]

- **Regulation P:** The Bureau should clearly state that data aggregators fall within the purview of its Privacy Rule, Regulation P. This would require data aggregators to provide disclosures to consumers about how data aggregators collect, store, and share any of their data as well as how it is safeguarded. This would help fill a critical gap that currently exists that puts consumers at a serious disadvantage. By furnishing the same disclosures as those supplied by other financial institutions, consumers would be better informed about how their data is collected and used. Most important, it would put them on notice about how data aggregators share that information with third parties. That would provide the needed transparency to help consumers make appropriate decisions and help them understand how their data are

---

8 15 U.S.C. § 6809(3).

9 12 U.S.C. § 1843(k). *See* 12 C.F.R. § 380.8(b)(3)(N)(1) Providing data processing, data storage and data transmission services, facilities (including data processing, data storage and data transmission hardware, software, documentation, or operating personnel), databases, advice, and access to such services, facilities, or databases by any technological means, if the data to be processed, stored or furnished are financial, banking or economic.

10 FTC Safeguards Rule, 16 C.F.R. § 314.3.

being used. In today's environment, that is critical knowledge that they lack without such notice.

- **FTC's Safeguards Rule:** At the same time, the Bureau should work with the FTC to clarify that data aggregators are subject to the FTC's Safeguards Rule. Ensuring that data aggregators are subject to GLBA and the data security requirements of the Safeguards Rule may not eliminate all regulatory gaps. In large part, this is due to the fact that FTC does not examine for compliance and instead relies on consumer complaints to identify problems. As discussed further in section V, this can be partially addressed by the Bureau identifying those data aggregators that are "larger participants" and subject to supervision by the Bureau.

  Also significant is the fact that the FTC Safeguards Rule does not require data aggregators to notify consumers or their banks in the event of a breach, depriving either party of the opportunity to take protective action. Moreover, unlike the data security standards that apply to banks, the Safeguards Rule does not outline the steps that an institution must take when a breach has occurred. ABA believes that these additional gaps should be addressed to ensure that customers are protected. At the same time as consumers are notified, ABA also believes it is critically important to require notice be provided to the financial institutions that created the data that might have been subject to compromise; failure to alert others in the data chain will not adequately protect consumers. We urge the Bureau to encourage the FTC to revise the safeguards rule to address these gaps.

Simply put, GLBA has set base standards that should apply equally and consistently to data aggregators as they do to any financial institution. There exist gaps in regulation today that the Bureau has the authority to address. Thus, ABA strongly urges the Bureau to exercise its authority under GLBA to ensure that consumer financial data retains its protected status throughout the data's lifecycle, ensuring consumers' data is protected consistently regardless of where the data originated, where it is transferred, and the type of company using or storing the data.

IV. Data Aggregator Practices Limit Control, Lack Transparency and Expose Consumers to Risks

To put a fine point on the need for protection of consumer data throughout its lifecycle, it is useful to review some specific current practices in the consumer financial data market have the potential to undermine longstanding consumer trust in banks to keep their data safe, secure, and private. When consumers allow data aggregators to access their data they run the risk – often unknowingly – associated with moving their data out of the secure banking environment, where it is fully protected by law, and moving it into the data services market where it is not accorded appropriate protections.

More troubling is that a number of these non-bank consumer financial data service providers take the position that financial data are no different from any other form of data, and as such

ignore or avoid any protections that should be afforded it. Furthermore, the lack of transparency and control, and the liability limits asserted by the aggregator, all work to the consumer's disadvantage.

There is Little Transparency or Control Regarding What Data Are Accessed and How They Are Used

Today, when consumers provide their access credentials to a data aggregator, they are giving that company access to any information that is housed in their online bank account, and they give access for an unlimited period of time. There is little effort to inform consumers about the information being taken, how it is being used or shared, how often it is being accessed, and how long the aggregator will continue to access it.

Consumers assume that data aggregators take only the data needed to provide the service requested. However, too often it is not the case. Many data aggregators use the data for purposes beyond the specific service that the customer sought. Access to all data enables the aggregator to profit by selling the information to other third parties even though the customer neither knew about that potential use nor requested any additional services or marketing.

Scrapping additional data also exposes the consumer to greater risk. For example, our members report that a customer's bank account number is the first piece of data an aggregator takes when it enters the banks' systems. This number is of little use for services offering a consolidated view of one's finances, but exposes the consumer to significant risk if that number were to fall into the wrong hands.

Liability Limits Attempt to Shift Liability to Consumers

Data aggregators that allow customers to conduct transactions through the data aggregator site are generally liable for unauthorized electronic fund transactions made through their site. However, a number of data aggregators have attempted to shift liability onto customers by including strict liability limitations in their terms and conditions. Examples of this include Intuit, which limits its liability to $500,[11] while Personal Capital limits its liability to $100.[12] In addition, data aggregators do not clearly warn their customers that the banks holding their accounts are not liable for unauthorized transactions conducted through the data aggregator to whom they have provided their "access device" e.g., credentials.

---

[11] Mint, Terms of Use, Section 17, available at https://www.mint.com/terms. "Intuit shall in no event be responsible or liable to you or to any third party, whether in contract, warranty, tort (including negligence) or otherwise, for any indirect, special, incidental, consequential, exemplary, liquidated or punitive damages, including but not limited to loss of profit, revenue or business, arising in whole or in part from your access to the sites, your use of the services, the sites or this agreement, even if intuit has been advised of the possibility of such damages. Notwithstanding anything to the contrary in this agreement, Intuit's liability to you for any cause whatever and regardless of the form of the action, will at all times be limited to a maximum of $500.00 (Five Hundred United States Dollars)."

[12] Personal Capital, Terms of Use, Section 16, available at https://www.personalcapital.com/content/terms-of-use/. "To the maximum extent permitted by applicable law, the liability of personal capital, its affiliates, licensors and agents to you shall not exceed one hundred U.S. dollars ($100)."

Aggregated Data Are an Attractive Target for Criminals

The risks to consumers should not be minimized. First, the sheer volume and value of the aggregated data make data aggregators a priority target for criminals, including identity thieves. This is because data aggregators collect and share information from multiple financial institutions which is a vast expansion of the information held at any one bank. Thus, data aggregators may have the financial information, including account credentials, for the accounts across a consumer's entire financial portfolio. Through a single source, the criminal may gain access to the consumer's checking and savings accounts, retirement accounts, certificates of deposits, credit cards, brokerage accounts, and insurance products. Also, increasingly data aggregators have the ability to conduct transactions, such as sending remittances, on behalf of consumers. This rich reward for a single hack, either of an aggregated database of personally identifiable information or of a single consumer's multiple accounts, makes data aggregators an attractive target for criminals. They obtain the key not to just a single room, but the key ring with keys to all the rooms.

Second, the impact on the consumer in the event of a compromise can be far greater than a single-financial institution compromise. With the consumers' credentials and account information, criminals may drain deposit accounts, liquidate stocks, and max out credit cards. Even if consumers are ultimately reimbursed, they may suffer crippling inconvenience from even a temporary loss of access because the unauthorized access involves all their financial accounts. They may have no access to funds for day-to-day living. Important payments may be returned unpaid, stocks may be sold at disadvantageous prices, and schedules and peace of mind will be upended as they attempt to recover their assets.

Third, consumers may suffer losses if the data aggregator is unwilling or lacks resources to reimburse the consumer. Under federal law, banks are not liable for unauthorized transactions made by the data aggregator or its employees to whom the consumer has provided the "access device," e.g., credentials to access the account and transfer money electronically. Regulation E, which implements EFTA, provides that consumers generally are not liable for unauthorized electronic fund transfers.[13] An "unauthorized electronic fund transfer" is a transfer by someone other than the consumer without actual authority to make the transfer and from which the consumer receives no benefit.[14] The term does not include transfers "by a person who was furnished the access device to the account by the consumer, unless the consumer has notified the financial institution that transfers by that person are no longer authorized."[15] The Official Staff Commentary further explains that if the consumer furnishes an access device and grants authority to a person who exceeds that authority, the consumer is liable unless the consumer has notified the financial institution that transfers by that person are no longer authorized.[16]

Thus, banks are not liable for unauthorized transactions made through the data aggregator. If a data aggregator is unable or unwilling to reimburse the consumer, the consumer suffers the loss.

---

13 12. C.F.R §1005.6.

14 12. C.F.R. §1005.2(m).

15 *Id*. at §1005.2(m)(1).

16 *Id.* at §1005.2(m) cmt 2. The aggregator might be liable under Regulation E, but only if it allows consumers to transfer funds through the aggregator.

Finally, it is not only the ability to access assets that presents consumer risk. Even if the criminal is limited to viewing account information, the mere knowledge of a person's financial assets provides useful information to criminals to identify more efficiently whom to target for scams. The greater their assets, the more attractive the victims. Knowledge of victims' assets is also useful in perpetrating the scam. Victims may be tricked into believing the criminal is legitimate. Knowledge of additional assets and accounts may be used to "persuade" victims to transmit additional funds.

V. The Bureau Should Address the Consumer Vulnerabilities and Risks

In addition to clarifying that GLBA applies to data aggregators, we urge the Bureau use its existing regulatory authorities as follows to address the vulnerabilities and risks highlighted above.

1. The Bureau should clarify that data aggregators are "service providers"[17] for purposes of Regulation E and thus liable for unauthorized electronic fund transfers that exceed the consumer's liability under Regulation E.

Under §1005.14 of Regulation E, a person that provides an electronic fund transfer service to a consumer is generally subject to Regulation E, with certain modifications, if it (1) issues an access device that the consumer can use to access the consumer's account held by a financial institution and (2) has no agreement with the account-holding institution regarding such access.

Data aggregators that permit consumers to initiate electronic fund transfers from accounts held at financial institutions that do not have an agreement with the financial institution are "service providers" under Regulation E, as they issue "access devices"[18] that may be used to permit electronic fund transfers to and from the account. As service providers, they are liable for unauthorized transactions under Regulation E as well as certain other provisions.

Imposing liability for unauthorized transactions under these circumstances is appropriate and fair. The data aggregator is in the best position to control the risk of unauthorized transactions conducted through its system. In contrast, the financial institution holding the account has no relationship with the data aggregator, no knowledge of, and no power over the data aggregator's security system. This approach is consistent with payment system laws which generally assign liability to the party that is in the best position to avoid a loss and manage the risk of a loss. Indeed, it is for these reasons that Regulation E assigns liability to service providers.

Moreover, other provisions related to service provider responsibilities support classifying data aggregators as service providers under Regulation E. These include requirements related to

---

[17] "Service provider" under Regulation E is a person that provides an electronic fund transfer service to a consumer but does not hold the consumer's account. The term is unrelated to "service providers" subject to vendor management requirements, for example.

[18] Under §1005.2(a) of Regulation E, "Access device means a card, code, or other means of access to a consumer's account, or any combination thereof, that may be used by the consumer to initiate electronic fund transfers." Some banks may offer credentials that allow a person to view account information but not transfer money. Additional or different credentials may be required to transfer money.

error resolution, disclosures, the prohibition against the issuance of unsolicited access devices, and change in terms notices.

ABA believes that data aggregators providing electronic fund transfer services are service providers under Regulation E. To avoid any ambiguity, we urge the Bureau to confirm this in the regulation or official commentary.

2. The Bureau should exercise its authority under Dodd-Frank Act §1024 to identify "larger participants" in the market for consumer financial data that are subject to supervision by the Bureau.

As discussed in section III above, data aggregators are subject to GLBA, but their compliance with its privacy and security obligations is not clear and, more important, is not subject to supervision or regular examination.

A cornerstone of Title X of the Dodd-Frank Act was the authority given to the Bureau 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."[19] 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 Bureau. This is especially important for data aggregators, given the sensitive consumer financial information they store and process.

As noted in the Request for Information, the bulk of the data processing in this area is managed by a select group of large companies. Accordingly, we urge the Bureau to initiate expeditiously 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 to and examination by the Bureau. Once the Bureau has imposed supervisory authority over the larger data aggregators, the Bureau can better monitor – and react to – risks to consumers in this rapidly evolving marketplace.

Despite the fact that §1024 allocates supervisory resources only to "larger" market participants, we believe that the possibility of oversight should encourage compliance efforts that might otherwise be lacking in entities that currently fall below the applicable larger participant threshold, but believe that their growth may make them subject to the Bureau's supervisory and record-keeping requirements in the future. Furthermore, even the smallest data aggregators that choose not to follow existing laws and regulations and are engaged in conduct that poses risk to consumers may be subject to the Bureau's supervisory authority under Dodd-Frank Act §1024(a)(1)(C). That section provides that a nonbank covered person of any size, operating in any market for consumer financial products and services may become subject to the supervisory authority of the Bureau because it "is engaging, or has engaged, in conduct that poses risk to

[19] 12 U.S.C. §5511(b)(4).

consumers with regard to the offering or provision of consumer financial products or services."[20] We strongly encourage the Bureau to exercise this authority.

3. The Bureau's Office of Financial Education should develop and implement a consumer education campaign to inform consumers about the risks, responsibilities, and choices associated with use of data aggregation products and services.

As discussed above, many consumers are unknowingly authorizing data aggregators to pull non-public, personal financial data from a bank's servers where it is accorded robust use and security protections, and they are releasing it into a data services market in which baseline consumer protection laws and regulations may be ignored or avoided. Few consumers are aware of the consequences of giving their access credentials to a third-party, namely that these practices can shift loss protection under Regulation E. Nor are they aware that data aggregators collect and transfer not only the data necessary for the particular fintech product or service the consumer sought to use, but the data aggregator often takes more information than needed and as much information as possible. Similarly, consumers may not be aware that data aggregators copy and store the data and, in some instances, may make use of or resell the data for other purposes.

As discussed, first and foremost, ABA recommends that the Bureau close regulatory gaps using its authority under GLBA and Regulation E and subject larger participants in the market for consumer financial data to regular supervision. However, taking those steps will take time and will not address completely the market and information failures that present risk to consumers. Therefore, we also encourage the Bureau's Office of Financial Education to develop and implement a consumer education campaign to inform consumers about the risks, responsibilities, and choices associated with use of data aggregation products and services.

4. The Bureau should exercise its authority under Dodd-Frank Act §1032 to prescribe rules to ensure that the features of any consumer financial product or service are fully, accurately, and effectively disclosed.

In a related vein, Dodd-Frank Act §1032 authorizes the Bureau to "prescribe rules to ensure that the features of any consumer financial product or service, both initially and over the term of the product or service, are fully, accurately, and effectively disclosed to consumers in a manner that permits consumers to understand the costs, benefits, and risks associated with the product or service, in light of the facts and circumstances."[21]

As discussed above, informed consumers are empowered to make appropriate and safe choices regarding access to their financial records—choices that offer the possibility to improve their control over their finances. ABA recommends that the Bureau use its rulemaking authority under §1032 to ensure that consumers are informed of the costs, benefits, and risks associated

---

[20] *Id.* at §5514(a)(1)(C).

[21] 12 U.S.C. §5532. *See also* 12 USC §5511(b)(1) & (2) (Requiring the Bureau to ensure that, "consumers are provided with timely and understandable information to make responsible decisions about financial transactions" and that "consumers are protected from unfair, deceptive, or abusive acts and practices.")

with their use of data aggregation products and services. Moreover, we encourage the Bureau to engage industry (banks, data aggregators, and end-user companies) and consumers in the design and testing of the disclosures as well as the timing and manner of delivery.

In particular, consumers should be provided with disclosures that provide information comparable to that provided by banks regarding the collection, use, and sharing of non-public personal information. As discussed above, under GLBA and its implementing regulations, financial institutions notify consumers about the consumer's non-public personal information that the bank collects, when that information might be shared, and how to request that certain information not be shared. Even more important for this discussion, consumers are notified about the steps taken to protect their information and, if there is a breach, provided additional notice about the breach and the steps the financial institution is taking and those the consumer should take.

In addition, the Bureau should ensure that data aggregators provide information clearly explaining which parties are liable for unauthorized transactions and their respective responsibilities. For example, clear and conspicuous notices should reflect the data aggregator's liability and responsibilities as service providers under Regulation E. Notices should also explain that banks are not liable for unauthorized transactions made through or by the data aggregator.

Closing Gaps Will Facilitate Safe Access More Effectively Than Action Under §1033

ABA recommends that the Bureau use its authority to address the regulatory gaps discussed above to promote the goals enumerated in the RFI. We believe that by clarifying data aggregator responsibility for maintaining the privacy and security of consumer financial data –including imposing breach notification obligations, confirming liability assignments under Regulation E, subjecting larger data aggregators to supervisory oversight, and educating consumers about the choices – responsibilities and risks presented will address emerging consumer protection concerns. In addition, taking these steps will encourage banks of all sizes to work with data aggregators and the fintech companies that use the data, facilitating financial innovation to the benefit of all.

We do not believe, however, that the Bureau can use Dodd-Frank Act §1033 to address consumer protection risks associated with data aggregation. §1033 authorizes the Bureau to facilitate consumer access to financial information, but that authority does not extend to regulation of third-party access to consumer financial information.

If implemented by rules written by the Bureau, §1033 of the Dodd-Frank Act will require a covered person to "make available to a consumer, upon request, information… concerning the consumer financial product or service that the consumer obtained from such covered person…" The information must be made available "in an electronic form usable by consumers" according to standards prescribed by the Bureau to promote the development and use of standardized formats "to be made available to consumers…"

Notably, §1033 only applies to consumers accessing their own information. The statute makes no mention of third party access to the information, even where the consumer has apparently granted authority. The plain language of the statute limits access to the account

information to the consumer. Had Congress intended to extend access to any person to whom the consumer had provided credentials (especially without the financial institution's knowledge), it would have so provided, as allowing access under such circumstances presents risks not present when consumers are given access to their own account information.

Accordingly, we do not believe the regulatory gaps presented can be addressed through implementation of §1033. Instead, ABA urges the Bureau to focus on measures such as those described above to clarify that data aggregators are subject to consumer protection rules, such as Regulation E and GLBA, ensure they are examined for compliance, and promote consumer education of consumer risks and responsibilities.

VI. A Better Way Forward

Banks are committed to giving consumers the ability to access and share their financial data in a secure, transparent manner that gives them control. This is not as easy as flipping a switch, as some have suggested, but banks and technology companies are working on the principles and technology to facilitate data. Banks and technology companies are collaborating to facilitate more secure access. In the past year significant progress has been made, in particular:

- The Center for Financial Services Innovation – a group that brings together traditional financial institutions and fintech startups – released a white paper detailing shared principles for data sharing.[22]

- Both JPMorgan Chase and Wells Fargo announced deals with Intuit to allow customers to share their financial data via API interfaces without requiring customers to give up their passwords.[23] [24]

- Both Citi and American Express announced investments in data aggregator Plaid (joining Goldman Sachs), citing the goal of "better access to clean, high-quality financial data, enabling innovation and a secure infrastructure for the financial services ecosystem." This collaboration could lead to more secure channels for customers to share their data.[25]

We believe that three core principles – security, transparency and control – should set the framework for how data is shared and how consumer data is treated. Principles will ensure that

[22] Center for Financial Services Innovation, Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration (Oct. 24, 2016), available at http://www.cfsinnovation.com/Document-Library/Consumer-Data-Sharing-Principles-A-Framework-for-I
[23] JPMorgan Chase, Chase, Intuit to Give Customers Greater Control of Their Information (Jan. 25, 2017), available at https://media.chase.com/content/pr/chase-intuit-give-customers-more-control
[24] Wells Fargo, Intuit Signs New Data-Exchange Agreement with Wells Fargo (Feb. 3, 2017), available at https://www.wellsfargo.com/about/press/2017/intuit-agreement_0203.content
[25] Plaid Unveils Investments by Citi Ventures and American Express Ventures (February 6, 2017), available at http://www.prnewswire.com/news-releases/plaid-unveils-investments-by-citi-ventures-and-american-express-ventures-300402531.html

consumers are treated fairly as new technologies develop and new innovations change the way data are being used.

Conclusion

Today, technology is fundamentally changing the way financial services are being delivered. Consumer financial data are more available and widely shared than ever before. ABA believes that innovations in financial services present tremendous value. This value is only realized when innovations are delivered in a responsible manner that maintains the trust that is critical to the functioning of our financial system. The focus on the consumer financial data market is important. We urge the Bureau to address the market as a whole and ensure that the data-sharing market is one that maintains consumers' trust in the financial system.

By fairly addressing both the opportunities and risks, we have the ability to give consumers innovative services that they can trust. Customers need security, transparency, and control to unlock the true potential of fintech and take charge of their financial future.

Sincerely,
Rob Morgan
Vice President, Emerging Technologies