February 4, 2021

Consumer Financial Protection Bureau
1700 G. Street, N.W.
Washington, DC 20552

Electronic Delivery to 2020-ANPR-1033@cfpb.gov

Re: Docket No. CFPB-2020-0034 / RIN 3170-AA78
Consumer Access to Financial Records

The Consumer Bankers Association[1] ("CBA") appreciates the opportunity to comment on the Consumer Financial Protection Bureau's ("Bureau" or "CFPB") Advanced Notice of Proposed Rulemaking (ANPR) concerning Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Section 1033").

In 2017, the Bureau released "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation" ("2017 Principles"), which expressed "the Bureau's vision for . . . a robust, safe, and workable data aggregation market that gives consumers protection, usefulness, and value."[2] The 2017 Principles detailed nine topics related to consumer-authorized access: access; data scope and usability; control and informed consent; authorizing payments; security; access transparency; accuracy; ability to dispute and resolve unauthorized access; and efficient and effective accountability mechanism. Since the release of the 2017 principles, industry participants engaged in a cooperative spirit to work towards creating not only a workable data aggregation market but a well-functioning, secure, data access ecosystem. CBA encourages the Bureau to take a balanced, cautious approach regarding Section 1033.

Against this background, CBA encourages the Bureau to undertake a risk-based assessment of that ecosystem and leverage that in developing its approach regarding Section 1033. This would include identification of gaps between the current data access ecosystem and the nine elements reflected in the 2017 Principles that include, among other things, instances of unfettered, unauthorized, and unsupervised third-party access to sensitive financial data. Absent clear and consistently applied standards for obtaining express consumer consent to the access and use of financial data, any consent may not be truly informed if it lacks a reasonable level of clarity. This data leaves the safety of a regulated financial institution without any requirement imposed upon the third-party, or any other subsequent data user or data processor, to keep the consumer's information safe from unauthorized access and use.

Banks have noted efforts to develop APIs limiting data access to that necessary to perform the expressly authorized aggregation services and to enter contracts with data aggregators obliging them to additional consumer protections, both with limited success. Financial institutions have virtually no leverage to require aggregators to agree to reasonable access and data security controls. Screen scraping and

[1] The Consumer Bankers Association partners with the nation's leading retail banks to promote sound policy, prepare the next generation of bankers, and finance the dreams of consumers and small businesses. The nation's largest financial institutions, as well as many regional banks, are CBA corporate members, collectively holding two thirds of the industry's total assets.

[2] Consumer Financial Protection Bureau, "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation" (Oct. 18, 2017) (available at: https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf).

aggregator storage of consumer passwords and pins are still highly prevalent, creating unnecessary and unacceptable data security risk. Data aggregator and other data user disclosures are sometimes confusing and buried in larger privacy policies, which consumers are not required to click through to establish an account with the third party. The downstream uses of the consumer data remain ambiguous to both banks and consumers.

In addition, the current data aggregator business model does not appear appropriate to access, store or to process consumer financial data. Unfettered access to consumer accounts (rather than limited access to account information) could subject consumers to significant losses in the event of a widespread breach into aggregator databases. In this scenario, it is unclear whether a consumer would bear those loses or whether the data aggregator would be held accountable.

Consumers deserve standardization in disclosures, consent, security and data usage requirements among aggregators and others to provide them with meaningful, informed consent. Financial institutions also need these standards to assess and to mitigate risks to the banks posed by data aggregator services.

With that being said, CBA recommends the Bureau analyze three critical areas to ensure consumers sensitive financial data is being used appropriately:

- Regulate All Participants in the Data Access Ecosystem
- Prioritize Consumer Control of their Data Security and Privacy
- Provide Consistent and Standard Data Security and Data Minimization Throughout the Entire Ecosystem

Regulate All Participants in the Data Access Ecosystem

Compliance with rules and regulations established to protect consumers is critical to a well-functioning data access ecosystem. The Bureau's 2017 Principles also recognized the critical balance of giving consumers the ability to share their data, while ensuring it remains protected. When consumer sensitive financial data is accessible by third parties who do not protect the information or access effectively, consumer risks is dramatically escalated. CBA urges the Bureau to propose a "Larger Participant Rule" to mandate supervision of segments of data users in the data access ecosystem – the data holder, data user, and the data aggregator. For significant players outside of the definition of a "Larger Participant Rule," CBA encourages the Bureau to exercise its authority pursuant to Section 1024(a)(1)(c) of the Dodd Frank Act to designate companies and to examine for compliance. Without federal oversight of all these participants, the consumer is at risk.

A regulatory framework can help the data access ecosystem more quickly innovate and collaborate. Access to consumers' account data has the potential to enable many products and services which will help consumers better manage their finances, but a sound financial system must incorporate a fair, level-playing field amongst all participants and the security and use minimization of consumer financial data. By addressing both the opportunity and risk of consumer access to data, the Bureau can facilitate innovation consumers can trust. Consumers need security, transparency, and control to unlock the true potential of financial innovation.

Prioritize Consumer Control of their Data Security and Privacy

Clear, Understandable and Actionable Disclosure to the Consumer

CBA urges the Bureau to inquire into whether the current consumer disclosures provided by data aggregators and other data users are transparent and meet the Bureau's standard set in its 2017 Principles. The Bureau needs to at least ask the following questions: "Does the consumer understand what is happening to their data? Is it clear to the average consumer when providing their credentials to a data user that a third-party may obtain your data? What are the data aggregators and data users doing with the consumer data? What is the purpose of the data collected? Will the data be subject to additional downstream uses and/or monetized? How may the consumer revoke access consent?"

A consumer's ability to control and maintain privacy over their financial information requires full transparency and informed, explicit consent. Clear, consistent language disclosures are critical to ensure consent is knowing and voluntary. The current disclosures provided by data aggregators and other data users do not provide the requisite transparency to fulfill the vision set forth by the CFPB in its 2017 Principles.

For instance, in Fall 2020, a bank filed a lawsuit alleging claims a data aggregator violated trademark agreements. According to the complaint, the data aggregator knowingly created a user interface which uses the bank's trademark, logos, and color scheme to mimic the bank's actual login page and deceive the bank's customers into believing they are entering their sensitive personal and financial information in the bank's trusted and secure platform. The bank also alleges the data aggregator stores consumer login information on its servers and mines the consumer data for transaction history and other information which can be sold to third parties. Examples like this case also raise concerns of unfair, deceptive, or abusive acts or practices ("UDAAP").

The resulting disclosures should explicitly communicate to consumers about any secondary or downstream use of their data. Unfortunately, in the current data access ecosystem, once consumers have granted permissioned access to their data, they are often unable to ascertain who holds their data. Banks have noted data aggregators use this access to gain real time account data regularly and frequently, even when the consumer no longer uses the service. Often, consumers mistake deleting an application with revoking consent or fail to change their login credentials. CBA urges the Bureau to promulgate specific, simple and consistent disclosure language for how a consumer's data will be used, shared or sold.

Consumer Reauthorization Requirement

CBA encourages the Bureau to look at the use of mandatory re-authentication requirements. Reauthorization would prevent data aggregators from having infinite unfettered access to sensitive consumer data information. In the current data access ecosystem, banks are unaware of when their consumers have either enrolled in or discontinued use of a data aggregator's services. As previously mentioned, banks have limited options since they cannot obligate aggregators to GLBA service provider restrictions because the aggregators are not vendors and often do not have contracts with the banks. For example, in the UK's open banking system, there is a 90-day reauthorization requirement for data aggregators to continue to access consumer data.[3]CBA member banks do not endorse any particular time frame for data reauthorization, rather, we encourage the Bureau to study the benefits of this option in the United States.

[3] 90 Day Re-Authentication, Open Banking Implementation Entity, https://standards.openbanking.org.uk/customer-experience-guidelines/ais-core-journeys/90-days-reauthentication/latest/ .

Provide Consistent and Standard Data Security and Data Minimization Throughout the Entire Data Access Ecosystem

CBA urges the Bureau to hold all participants in the data access ecosystem to the same or a materially comparable standard contained in the Gramm-Leach-Bliley Act ("GLBA") to hold or process consumer financial data. Consumer financial data is protected pursuant to GLBA when held by a depository institution. When consumers grant permissioned access to data aggregators, the sensitive data leaves the regulated and supervised environment of a bank and flows to the data aggregator. CBA member banks maintain the GLBA protections should continue to remain attached to the data throughout all entities in the data access ecosystem.

Since the data is no longer solely with a regulated and supervised bank, the sensitive data becomes more vulnerable to attack and misuse when in the possession of unregulated and unsupervised entities. This threat is intensified where, as here it is often unclear how any additional data holders or data processes secure and protect the sensitive consumer financial data. The Bureau should make clear data aggregators are subject to GLBA standards to prevent potential harm to consumers. CBA supports consumer access to data, but we believe the scope of Section 1033 should be limited to the data created and collected during the ordinary course of business. In addition to providing consumers products and services, banks through research and development create proprietary data sets which are beyond the scope of Section 1033.

Defer to Industry-Led Data Security Standards

The financial services industry, through industry standard-setting bodies, should continue to take the lead in developing the standards for consumer-authorized data access consistent with the Bureau's 2017 Principles. An industry-led approach is the most efficient way to facilitate both innovation and interoperability. Industry-led standards will also better facilitate a nimble and secure data access ecosystem which can quickly and effectively respond to new threats and capitalize on opportunities to consider emerging technologies.

Section 1033 of Dodd-Frank contemplates an industry setting approach. The law requires the Bureau "to prescribe standards applicable to covered persons to promote the development and use of standardized formats." While the provision requires the Bureau to prescribe consumer access to data standards, it also contemplates industry development of detailed and specific rules. This industry-led approach has been utilized by the Bureau to date and has provided the industry with the necessary flexibility to grow and innovate.

The industry has made significant progress in recent years in collaborating to develop standards for interoperability across the data access ecosystem. For example, the Financial Data Exchange ("FDX") has developed an application programming interface ("API") that can facilitate secure data sharing among all parties. The FDX API technical standard seeks to replace the practice of credential-based data access and screen scraping with tokenized access in concert with API-based data collection. API use will allow a consumer to be securely authenticated at their own financial institution and permission only the data the consumer chooses to share to ensure he or she can choose the type of data that is shared. This also permits the consumer's bank to ensure a consumer's consent to share information is terminated upon revocation. Other examples include: The Clearing House's Connected Banking Initiative, which advocates for new technology standards and infrastructure; Akoya, which provides consumers with more control and security when connecting their bank accounts to third parties; and Afinis, which furthers the work of

Nacha's Payments Innovation Alliance API Standardization Industry Group to advance standardization efforts across the financial services ecosystem through formal governance.

Prescriptive standards would impede industry flexibility to adapt to changes in technology. A Bureau led effort would likely include lag time between the emergence of new threats or opportunities and any regulatory response. CBA urges the Bureau to provide an overarching framework to encourage interoperability and wide adoption to industry standards.

Additional Issues to Consider

Data Aggregators are Not Bank Vendors

CBA believes the goal of a more secure, transparent data access ecosystem is to safely share consumer information. Bank vendor relationships traditionally refer to agreements between the bank and its service provider through written contractual agreement between both parties. However, in our current data access ecosystem this is not the case. Banks that contract with willing data aggregators and fintechs to effectuate the wishes of the consumer and to reduce risk by applying additional protections to consumer's data as it exits the secure banking environment.

Section 7 of the Bank Service Company Act ("BSCA") requires banks to notify their regulators of contracts or relationships with certain third-party service providers and to meet due diligence requirements. This position is intended to capture partnerships with third parties to deliver experiences to consumers. In this context, a partnership does not exist.

Ambiguity concerning the applicability of the BSCA to contracts with data aggregators could stifle adoption of more secure technologies, which provide additional protections for consumers.

Apply Liability Provisions to Applicable Data Aggregators and Fintechs

Pursuant to §1005.14 of Regulation E, an entity which 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 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 who conduct consumer electronic fund transfers without an agreement with the consumer's financial institution are providing a service subject to Regulation E. Pursuant to Regulation E, these third parties issue "access devices" which may be used by the consumer to access their accounts held by a financial institution. As service providers, they are liable for unauthorized transactions under Regulation E and also subject to certain other provisions, e.g., requirements related to error resolution, disclosures, the prohibition against the issuance of unsolicited access devices, and change in terms notices.

CBA supports imposing liability for unauthorized transactions to create a more secure and transparent data access ecosystem. This approach is consistent with payment system laws which generally assign liability to the party is in the best position to avoid a loss and to manage the risk of a loss. Indeed, it is for these reasons that Regulation E assigns liability to service providers.

Banks Do Not Furnish Credit Data to Aggregators

The Fair Credit Reporting Act ("FCRA") and its regulations create a massive framework of rules which govern consumer reports and the use of sharing of information related to those consumer reports. Whether

the requirements of the FCRA apply to a situation depends in large part on whether the information being shared meets the definition of consumer report and whether the organization sharing information meets the definition of a consumer reporting agency. Generally, consumer reports are primarily used to ascertain a consumer's credit worthiness for personal, family or household purposes.

In contrast, in the current data access ecosystem, the "purpose" of sharing permissioned data is not clear and FCRA should not apply to this activity. Thus, banks should not be considered furnishers for the purposes of sharing data with data aggregators or fintechs.

Coordinate with Other Banking Regulators in any Rulemaking

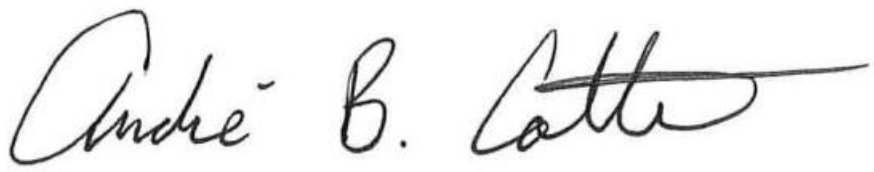
Implementation of Section 1033 has wide reaching implications for a bank, including regulatory considerations related to its safety and soundness obligations in the context of the sensitive nature of financial data it accesses and maintains. This has been acknowledged by the requirement contained in Section 1033 that the CFPB is to "consult with the Federal banking agencies and the Federal Trade Commission," when prescribing any rules.

Conclusion

CBA thanks the Bureau for the opportunity to comment on Section 1033 of the Dodd-Frank Act. We believe the Bureau should continue to take a principles-based approach to consumer access to data. However, we encourage the Bureau to ensure the security and transparency of the data access ecosystem. Data aggregators and data users should be regulated and held to a security standard appropriate for consumer's sensitive financial data. Most importantly, consumers deserve clear, plain disclosures from data aggregators and data holders which clearly explain and identify the use and location of their data, as well as a clear process for consumers to revoke consent for aggregator access. CBA believes a cohesive regulatory framework will help the data access ecosystem more quickly and safely innovate and collaborate.

If you have any additional questions or concerns, please do not hesitate to contact André Cotten at 202-552-6360 or at Acotten@consumerbankers.com.

Sincerely,



André B. Cotten
Assistant Vice President, Regulator Counsel
Consumer Bankers Association