



www.fdata.global/north-america

June 16, 2023

Comment Intake
Consumer Financial Protection Bureau
1700 G Street NW
Washington, D.C. 20552

SENT VIA ELECTRONIC MAIL TO DataBrokersRFI_2023@cfpb.gov

Docket No. CFPB-2023-0020

Re: Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information

The Financial Data and Technology Association of North America (“FDATA North America”) appreciates the opportunity to provide its perspectives in response to the Consumer Financial Protection Bureau’s (“CFPB” or “the Bureau”) Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information.

FDATA North America was founded in early 2018 by several financial technology firms whose technology-based products and services allow consumers and small and medium enterprises (“SME”) to improve their financial wellbeing. As the leading trade association advocating for customer-permissioned access to financial data, FDATA North America’s members include firms with a variety of different business models.

Collectively, our members provide more than 150 million American consumers and SMEs access to vital financial services and products, either on their own or through partnerships with supervised financial institutions. Regardless of their business model, each FDATA North America member’s product or service shares one fundamental and foundational requisite: the ability of a customer to actively permission access to some component of their own financial data that is held by financial services providers.

Overview

As a trade association that represents dozens of financial technology companies that are focused on enabling greater competition and choice in the financial services marketplace, we would suggest to the Bureau, in the strongest possible terms, that third-party providers of financial services that rely on consumer-permissioned data are not data brokers, and therefore should be exempt from any Bureau rulemakings, guidance, or other actions it may consider in the data brokerage space.



www.fdata.global/north-america

Consumer-Permissioned Third-Party Financial Service Providers are Not Data Brokers

The deployment of financial technology applications within the financial services ecosystem has fostered the ability of consumers and SME owners to use their financial data to make payments, manage their budgets, access capital, increase their savings, and invest safely and securely. The empowerment consumers receive under this open finance framework provides them with the opportunity to improve their financial wellbeing, access value-based services, and take control over which entities have access to their financial data. Achieving this outcome requires transparent, uniform consent requirements which all stakeholders must comply with to ensure that end users understand precisely what data they are providing to a third-party service provider. This also includes the ability to revoke that consent at any time. A supervisory framework under which data aggregation platforms are subject to CFPB examinations has the potential to provide for this outcome. The Bureau is currently working to formalize these standards via a rulemaking under Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("the Dodd-Frank Act"); an effort that FDATA North America has strongly supported since our inception. To the extent the CFPB undertakes future rulemaking of data brokers, FDATA North America would respectfully offer that the Bureau should distinguish entities which do not receive consent to collect customer information, from customer-permissioned data recipients, which do receive customer consent, to avoid unnecessary interference and confusion with a rulemaking that is already underway.

End-to-end customer control and transparency is an inherent feature of the customer permissioned financial data marketplace. In many cases, financial institutions, in partnership with data aggregation firms, present to their customers a dashboard that enumerates the various data connections they have established to their accounts and what data elements they have permissioned to fuel the use cases they have connected. When account connectivity is first established with a third-party service provider, aggregation platforms presented significantly more conspicuous disclosures regarding what data was being accessed, for what purpose, and for what length of time. It is in the customer's and ecosystem's best interest to understand who is accessing what data and for what purposes, and FDATA North America's members are, in partnership with financial institutions, providing innovative solutions in this regard today. The customer's control of their data in the customer-permissioned financial data marketplace, which we anticipate will be enshrined in an eventual Section 1033 rulemaking, is therefore a key feature of the ecosystem in which third-party financial providers and data aggregation platforms operate today.

It is also important in the context of the Bureau's RFI to distinguish between the type of data collected by some data brokers compared to consumer-permissioned financial transaction data collected by third party financial providers and data aggregation platforms. Customer-permissioned third-party providers of financial services can only make use of the specific data fields to which the customer has deliberately granted them access.



www.fdata.global/north-america

To be clear, FDATA North America and its member companies that rely on consumer-permissioned access to financial data strongly support the creation of federal data privacy standards by Congress that are consistently applied to all market participants and designed and implemented with the consumer's best interests in mind. FDATA North America and its member companies developed and published a set of privacy principles earlier this year, which we hope will inform legislative consideration of a federal data privacy regime. In our principles, FDATA North America defined customer-directed data as financial data that is collected or shared in accordance with a clear affirmative action by or request from an end user or their authorized agent, rather than data collected passively, such as data that may be collected automatically through pixels or cookies as a consumer navigates through web pages. For data to be considered customer-directed, our principles further assert that the end user must also have full utility over any non-proprietary data element for which a data holder holds about them. And critically, the end user must have the ability to opt-out of future use of their data at any time. FDATA North America's member companies abide by these principles today and, in so doing, provide end users with significant transparency into and control over how their data is being accessed.

Similarly, FDATA North America and its members believe that data minimization is also central to customer protection and security in the financial services ecosystem. No third party should have access to any financial data element permissioned by a customer that is not required to fuel the use case for which that customer has opted in. This should be central to any supervisory regime the Bureau establishes for financial data aggregation firms as it contemplates a Section 1033 rulemaking, as these firms provide the data connectivity for the thousands of third parties in the financial technology ecosystem. Supervision of aggregators would provide the Bureau with the ability to ensure data minimization requirements are adhered to by market stakeholders and would provide the CFPB with direct oversight of customer-permissioned data aggregation platforms.

Conclusion

For all the reasons stated above, FDATA North America urges the Bureau to distinguish customer-permissioned third-party providers of financial services from data brokers for the purpose of any future CFPB rulemaking or guidance. The Bureau's forthcoming rulemaking under Section 1033 of the Dodd-Frank Act will provide significant customer control and transparency into how their data is being accessed and shared in the customer-permissioned financial data ecosystem today. To the extent the CFPB ultimately pursues future rulemaking or guidance regarding data brokers, inclusion of customer-permissioned data third-party providers of financial services would serve only to introduce unnecessary regulatory complexity into a market that is already preparing for regulation under a Section 1033 rulemaking.

On behalf of FDATA North America, thank you for your consideration of our submission in response to this Request for Information and for your continued work on this critical issue.

Sincerely,



www.fdata.global/north-america

A handwritten signature in black ink, appearing to read "St Boms".

Steven Boms
Executive Director