Financial Data and Technology Association

http://www.fdata.global/north-america

May 21, 2020

The Honorable Maxine Waters
Chairwoman
Committee on Financial Services
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Patrick McHenry
Ranking Member
Committee on Financial Services
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairwoman Waters and Ranking Member McHenry,

I am writing to you on behalf of the Financial Data and Technology Association of North America (FDATA North America) regarding the critical issue of financial data privacy. Under your leadership the committee has spent significant time focused on this important matter. As consumers and small businesses increasingly engage with financial service providers digitally, ensuring that customers are protected – and empowered – when accessing their financial data is a top priority for the financial technology and customer-permissioned aggregation firms that comprise FDATA North America's membership.

FDATA North America and its members are expert voices on financial data sharing and consumer privacy and we hope that you will utilize us as a resource as the committee explores legislative efforts on this topic. As the leading trade association advocating for consumer-permissioned, third-party access to financial data globally, we believe that the most effective way to ensure data privacy is to give consumers and small businesses the tools to control their financial data. Having been integrally involved in the deployment of financial data privacy and empowerment regimes in the United Kingdom, Europe, Australia, Canada, and several other jurisdictions, FDATA North America can credibly assert that under open finance regimes consumers can experience both full access to their data and certainty that their data is used only in the way they intend. .

Every financial technology tool requires that its customers provide access to his or her financial data to provide a valuable service or product to that customer. While this exchange of customer-permissioned data to a third party through a data aggregation platform may seem novel, it is essentially the modern-day equivalent of a customer taking a shoebox filled with receipts and bank statements to a provider of her choosing. In the United States, the question of how, technologically, the financial tool may access the customer's financial data with her permission is, under current market and policy structure, solely at the discretion of the customer's financial institution. While some financial institutions have created Application Programming Interfaces (APIs) to facilitate the flow of customer-permissioned data access to

third-party service providers, the overwhelming majority of financial data access in the market today – perhaps as much as 90 percent – is provided by credential-based "screen scraping."

As you know, screen scraping is a technology process through which third parties access read-only financial data with users' consent via a financial institution's native online banking environment. This mode of aggregation is often – but not always – enabled through credential-based authentication; a practice in which users entrust their login credentials to the third-party aggregator under a legally binding contract and subject to applicable law to enable read-only access to their financial data. Once authenticated, a screen scraping data access method sees the deployment of software to read the data from the user's online banking environment required to power the application or service they are using.

APIs are another technology that allows customers to share their financial data with financial service providers of their choosing. While accessing data through APIs is unquestionably faster and more reliable than screen scraping, much of the financial data critical to facilitating users' ability to take advantage of third-party tools that can provide them with valuable financial benefit cannot today be accessed through APIs because financial institutions have not yet built and deployed APIs at scale. While the financial services industry is naturally evolving towards increased usage of API technology to share data, the transition will take time before data parity for API access methods can be achieved as compared to screen scraping methods.

FDATA North America strongly urges the committee to resist calls to mandate or limit the ability of consumer and small businesses to access their financial data using any individual technological access method, as doing so would have dire financial access implications. At the request of the Consumer Financial Protection Bureau, FDATA North America last year conducted an assessment on the implications of a mandated transition from screen scraping as a data access to API-only data access. The data showed that if screen scraping were prohibited and only API access was made available, nearly two billion customer financial accounts in the United States would immediately lose functionality due to the inability of those applications to connect to users' financial data critical to fueling the financial application for which the customer had enrolled. One year later, in an economic environment in which consumers and small businesses are more dependent than ever before on their ability to manage their finances digitally, a restriction on financial access of this magnitude would be disastrous.

Despite the significant implications of mandating or limiting financial data access methods, FDATA North America offers that, to the extent the committee does contemplate mandating or limiting particular financial data access methods, it is critical that the same data be made available through whatever technology is mandated as is currently available to consumers and small businesses through screen scraping. Any other outcome would be a net loss of consumer control over their finances, with direct impact on consumers' financial well-being.

As consumers increasingly desire access to and privacy of their financial data while utilizing technology-powered tools to manage their finances, our members are united behind the principle that consumer electronic financial data access and protection are fundamental rights and a market-driven imperative. This concept was formalized in Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the Dodd-Frank Act), which assures consumers electronic access to their financial data. Section 1033 of the Dodd-Frank Act recognizes that the deployment of financial technology applications in the financial ecosystem has fostered the ability of consumers and small business owners across the United States to use their own financial data to manage their budgets, access capital, increase their savings, and invest safely and securely, among many other use cases. By placing consumers and small businesses – the owners of financial data – at the center of the framework, end users are given complete control over their data. Along with the opportunity to improve their financial wellbeing by empowering them to use their data for the products and services of their choice, this construct provides consumers the ability to manage their own privacy by controlling which entities have access to their financial data and how that data can be used.

As you approach legislative solutions for improving consumer data privacy in the financial services industry, we hope that you will take a holistic, evidence-based approach that recognizes the importance of data utility and portability for consumers and small businesses. Doing so will provide for improved financial data protection but, critically, also facilitate consumer and small business data control and empowerment. Our members strongly believe in the ability of technological innovation to empower consumers by increasing competition and providing broader access to technology-based financial tools that drastically improves financial wellbeing, while adhering to best-in-class privacy and data security standards. Americans are more dependent than ever before on digital financial services not only to improve their financial wellbeing, but to manage it safely amidst a global health crisis, in a policy environment that never envisioned data – and not just consumer funds – as an important asset. Accordingly, as the committee considers the best way to protect consumer data privacy we wish to emphasize that the best way to protect consumer data privacy is to assert the legal right of the consumer to permission his or her own data.

Financial Data and Technology Association

http://www.fdata.global/north-america

Of course, to the extent that FDATA North America may be able to provide any additional information, we would be delighted to do so.

Sincerely,

Steven Boms
Executive Director
FDATA North America

Cc: House Financial Services Committee Members