Testimony of Steven Boms

President, Allon Advocacy, LLC
On Behalf of the Consumer Financial Data Rights Group

before the

Committee on Banking, Housing, and Urban Affairs

United States Senate

Fintech: Examining Digitization, Data and Technology

September 18, 2018

Introduction

Chairman Crapo, Ranking Member Brown and members of the Committee, thank you for the opportunity to testify today on behalf of the Consumer Financial Data Rights, or CFDR, Group. The CFDR Group is a consortium of nearly 50 financial technology ("fintech") companies, including financial data aggregation companies and end user-facing technology tools, on whose services more than 100 million consumers and small businesses collectively depend for access to vital financial services and wellness applications that serve them at every stage of their financial lifecycles. CFDR Group member-companies provide, for example, automated savings services, no-fee credit cards, investment advisory services, retirement savings advice and critical small business capital. In the complex and often opaque financial services ecosystem, the CFDR Group strives to be the voice of consumers and small businesses before policymakers and market stakeholders alike.

My testimony today also provides the perspective of the Financial Data and Technology Association ("FDATA") of North America, a trade association for which I serve as Executive Director. FDATA North America is comprised of several financial services providers, some newer entrant fintech firms and some incumbent, traditional providers, united behind the notion that standardization of consumer data access is both a fundamental consumer right and a market-driven imperative. FDATA North America is a regional chapter of FDATA Global, which was the driving force for Open Banking in the United Kingdom and which continues to provide technical expertise to regulators and policymakers in London, to the European Commission, and to regulatory bodies internationally contemplating many of the same issues identified in the Department of the Treasury's ("the Department" or "Treasury") report released on July 31, *A Financial System That Creates Opportunities: Nonbank Financials, Fintech, and Innovation*.

The CFDR Group and its members consulted frequently with the Department as it considered the current state of the fintech market, the consumer and small business benefits it provides to Americans today, and how best to harness innovation in the fintech ecosystem moving forward while ensuring that consumers, small businesses and the financial system itself are well protected. The CFDR Group's engagement with Treasury was principally focused on the crucial issue of consumer-permissioned financial data, which ultimately was an area of emphasis in the Department's report.

Ultimately, any provider of a technology-based financial tool, whether that provider is a fintech firm or a longstanding market incumbent, depends on the ability to access and utilize, with the consumer's or small business' express permission, elements of that customer's financial data to offer its products or services. Financial data, including, for example, balances, fees, transactions, and interest charges, are essential to facilitating the technology tools on which millions of Americans depend. These data elements are typically held at the financial institution with which that customer holds a checking, savings, and/or lending account. Before providing an overview of how this data exchange works today in the United States, I would first like to underscore the immense need that the technology-based tools offered by CFDR Group and FDATA North America member firms are fulfilling.

The State of U.S. Consumer Finances

Although the U.S. economy is performing well from a macroeconomic standpoint, there are unquestionably significant numbers of Americans who are being left behind and are financially invisible. The level of credit card debt in the United States is historically high and, earlier this year, exceeded $1 trillion for the first time ever, with the average American household holding approximately $8,200 in credit card debt.[1] About half of American consumers have no retirement savings at all, and of those that do, the average retirement account balance is about $60,000.[2] Approximately one-third of American adults have sufficient savings to last comfortably for more than a few months during their golden years.[3]

The crisis, of course, is not limited only to an accumulation of debt or a lack of retirement savings. The Federal Reserve Board of Governors determined earlier this year that 40 percent of American consumers could not afford a surprise $400 expense without either selling an asset or taking on additional debt.[4] And, unsurprisingly, many of us do encounter these surprise expenses. According to a recent study by CIT Bank, while half of Americans experience a financial emergency, such as a major health event or an unforeseen home repair, every year, more than one in four do not save for these unexpected events.[5]

It is no wonder, then, that 85 percent of Americans report feeling anxious about their financial state, with more than two-thirds believing that their financial anxiety is negatively impacting their overall health.[6]

Compounding this economic predicament is the growing complexity of most consumers' and small business' relationships with the American financial system. The vast majority of Americans have multiple different accounts across a variety of products providers. The most basic, fundamental first step towards financial health — simply understanding what one has and what one owes — is often intimidating and logistically difficult for all but the most financially savvy. The technology-powered tools on which millions of Americans have come to depend, provide intuitive, accessible platforms that enable even the least financially savvy among us to manage their finances and improve their economic outcomes. In addition to allowing Americans to see the totality of their financial accounts in one place, these applications empower consumers and small businesses to find lower loan rates or better loan terms, to avoid predatory products and services, to compare fees across different product offerings, to receive personalized

[1] Comoreanu, A. (2018, June 11). Credit Card Debt Study: Trends & Insights. Retrieved from https://wallethub.com/edu/credit card-debt-study/24400/

[2] Morrissey, M. (2016, March 3). The State of American Retirement: How 401(k)s have failed most American workers. Retrieved from https://www.epi.org/publication/retirement-in-america/

[3] 1 in 3 Americans Have Less Than $5,000 in Retirement Savings. (2018, May 8). Retrieved from https://news.northwesternmutual.com/2018-05-08-1-In-3-Americans-Have-Less-Than-5-000-In-Retirement-Savings

[4] Report on the Economic Well-Being of U.S. Households in 2017. (2018, May 22). Retrieved from https://www.federalreserve.gov/publications/files/2017-report-economic-well-being-us-households-201805.pdf

[5] Summer Survey: Trends on saving for life's planned and unplanned events. (2018, August 1). Retrieved from https://bankoncit.com/blog/2018-summer-savings-survey/

[6] Planning & Progress Study 2016. (2016, June 8). Retrieved from https://news.northwesternmutual.com/planning-and-progress-study-2016

investment and wealth management advice, to find and secure capital that otherwise may not be extended, or to take advantage of budgeting and savings tips to secure their financial future.

This of course presumes that one has access to the system in the first place. Twenty percent of adult Americans are underbanked by the traditional financial services system and almost nine million American households are entirely unbanked.[7] For these consumers, third-party, technology-based tools can provide vital, affordable access to a financial system that has left them behind.

Regardless of the use case a consumer or a small business wishes to leverage, and irrespective of whether that technology-powered tool is offered by a fintech firm or a traditional financial services provider, the lifeblood of these tools is user-permissioned data access: the right of the consumer or small business to affirmatively grant access to the third party of their choice to connect to or see the financial data required to provide them the product or service for which they have provided their consent.

The State of Consumer-Permissioned Financial Data

Usage of third-party, fintech tools in the U.S. is widespread: by 2017, 87 percent of consumers preferred to adopt a fintech application rather than use a product or service offered by a traditional financial services provider.[8] To gain access, with the consumer's or small business' consent, to their customer's financial data in order to provide their products or services, the vast majority of technology-based tools retain contractual relationships with financial data aggregators, such as Envestnet Yodlee, Quovo, or Morningstar ByAllAccounts, all of which are members of the CFDR Group. These aggregators, which have built data connectivity to thousands of U.S. financial institutions over many years, function as technology service providers for the consumer or small business-facing applications. Once the consumer or small business has affirmatively provided their consent to the application that they wish to utilize, that consent is transmitted to their financial institution and they are authenticated. Upon authentication, the aggregator utilizes one or more methods of data consumption to capture the financial data permissioned by the end user that is required to deliver the use case requested and delivers it to the application provider. The application provider then uses this data to provide its service or product to the consumer or small business.

Because there are no overarching statutory, regulatory or market standards in the United States with regard to consumer or small business authentication, or with regard to the data consumption protocol used by aggregators to transmit the end user's data, with their permission, to their application of choice, there are several different methods used in the ecosystem today. To authenticate, end users typically provide their online banking credentials, either to the third-party application provider delivering them the service or product they have selected, or, through redirection, to their financial institution, which in turn issues an access token to the third party

[7] Financial inclusion in the United States. (2016, June 10). Retrieved from https://obamawhitehouse.archives.gov/blog/2016/06/10/financial-inclusion-united-states
[8] EY FinTech Adoption Index 2017. (2017, June 28). Retrieves from https://www.ey.com/Publication/vwLUAssets/ey-fintech-adoption-index-2017/$FILE/ey-fintech-adoption-index-2017.pdf

and the aggregator with which it partners. Once the consumer or small business is authenticated, the aggregator may use any of several data consumption methods to retrieve the financial data required for the use case. Some financial institutions have created direct feeds, such as Application Programming Interfaces ("APIs"), specifically for aggregators and third parties to utilize for the purpose of providing products or services to their customers; however, the vast majority of U.S. financial institutions have not. The significant capital investment required to build and maintain these feeds typically results in only the largest U.S. financial institutions deploying them. In the case where no direct data feed is available, aggregators employ proprietary software to retrieve the data required for the use case from the end user's native online banking environment. This data consumption method is colloquially referred to as "screen scraping."

I note here a critical issue that underlies the entire fintech ecosystem's ability to continue to deliver the products and services on which many consumers and small businesses now rely: There is no legal requirement in the United States stipulating that a financial institution must make the consumer's or small business' financial data it holds available to a third party in the event their customer provides affirmative consent for the institution to do so. Accordingly, a consumer's or small business' ability to take advantage of the benefits offered by third-party, technology-based tools rests almost entirely with the inclination of their financial institutions to allow them to do so. Not all financial institutions are disposed to allow third-party tools, some of which compete directly with their own products and services, complete access to their customers' data. The Treasury's report notes, for example, that "access [to financial data] through APIs was frequently and unilaterally restricted, interrupted, or terminated by financial services companies."[9] In many cases, these APIs also may not provide the full suite of data required by technology-powered tools to deliver their products or services. The market is therefore fundamentally dislocated; the ability of U.S. consumers and small businesses to utilize third-party technology tools is dependent on the financial services provider(s) with which they do business, with disparate outcomes for Americans who bank with different financial institutions. The unevenness of this playing field could materially worsen as many large U.S. financial institutions seek to impose on consumers and small businesses their view of how the ecosystem should function in the form of bilateral agreements with aggregation firms.

The Bureau of Consumer Financial Protection ("BCFP" or "the Bureau") engaged in a year-long process to address this issue, which ultimately culminated in the release in October 2017 of nonbinding principles for consumer-authorized financial data sharing and aggregation.[10] Though the BCFP's engagement was earnest and well-intentioned, the principles it ultimately released did not meaningfully shape or change market behavior, both because they were not legally binding and because the Bureau declined to forcefully stake out a position regarding consumer-permissioned data access. The BCFP asserted, for example, that consumers "generally" should be able to use "trusted" third parties to obtain information from account

[9] *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation*. (2018, July 31). Retrieved from https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf

[10] Consumer Protection Principles: Consumer-authorized Financial Data Sharing and Aggregation. (2017, October 18). Retrieved from https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf

providers[11] but provided no further detail regarding these qualifiers. As a result of this ambiguity, and despite the BCFP's much-needed engagement in the market, the state of consumer-permissioned financial data access in the United States is not meaningfully different today than it was when the Bureau's nonbinding principles were released almost one year ago.

While policymakers in the United States have not issued any regulation specific to consumer-permissioned financial data access, regulators and legislators abroad have sought to harness innovation. As these other jurisdictions implement frameworks that harness innovation, the U.S. market is at risk of losing pace internationally with the development and delivery of new, innovative financial tools for consumers. There is, accordingly, "a huge risk the U.S. will fall behind, and with that a risk that jobs will go elsewhere."[12]

The United Kingdom's Open Banking regime, under which consumers can utilize authorized third-party tools without restriction, began its implementation phase earlier this year, as did Europe's Second Payments Services Directive, or PSD2. In Mexico, following a recently-passed new fintech law, the Bank of Mexico and the National Banking and Securities Commission ("CNBV") are in the midst of developing API standards that national financial institutions will be required to adopt in order to facilitate the use of third-party fintech tools. The Australian government has made public its intention to begin its implementation of an Open Banking regime in July 2019, and New Zealand, Canada and Mexico are not far behind.

In the preamble to its report, Treasury rightly notes that policymakers' engagement with the fintech ecosystem — and the decisions that are made by the financial regulatory agencies in response to the Department's recommendations, particularly with regard to consumer-permissioned data access — will have implications for U.S. global competitiveness.[13] Developments such as the announcement earlier this month of a pact between the Monetary Authority of Singapore and the Dubai Financial Services Authority to work collaboratively on digital payments and blockchain projects are becoming increasingly common. While the U.S. market continues to consider the most fundamental policy issues regarding innovation in financial services, policymakers in other jurisdictions are assertively creating well-regulated, innovative regulatory frameworks designed to attract and encourage large-scale innovation. The stakes are high: Globally, the fintech market attracted more than $31 billion in 2017, with the United States attracting more than half the investment in the market.[14]

Treasury Report Recommendations

Both the CFDR Group and FDATA North America strongly believe that the Department in its July report identified the key outstanding issues with regard to consumer and small business financial data access. I would respectfully highlight five of the Treasury recommendations for the Committee's consideration, as formalizing standards around these areas

[11] Ibid.
[12] Phillips, C. (2018, September 12). Remarks to the Exchequer Club of Washington. Speech, Washington, D.C.
[13] *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation*. (2018, July 31). Retrieved from https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf
[14] The Pulse of Fintech – Q4 2017. (2018, February 13). Retrieved from https://home.kpmg.com/xx/en/home/insights/2018/02/pulse-of-fintech-q4-2017.html

would significantly bolster the ability of Americans to utilize third-party technology tools to improve their financial wellbeing:

1. *The Bureau should affirm that for purposes of Section 1033 [of the Dodd-Frank Wall Street Reform and Consumer Protection Act], third parties properly authorized by consumers…fall within the definition of "consumer" under Section 1002(4) of Dodd-Frank for the purpose of obtaining access to financial account and transaction data.*

Treasury's assertion that the Dodd-Frank Act's inclusion of language in Section 1033 mandating that financial institutions provide their customers with electronic access to their data should be interpreted to "cover circumstances in which consumers affirmatively authorize, with adequate disclosure, third parties such as data aggregators and consumer fintech application providers to access their financial account and transaction data from financial services companies"[15] marks a significant step forward for consumers' and small businesses' financial rights. Though it may seem self-evident, because Section 1033 of Dodd-Frank provides that the BCFP has the authority to promulgate a rule to ensure end users have electronic access to their online data, and the Bureau has thus far declined to do so, Treasury's affirmation that the Dodd-Frank Act provides this right to consumers and small businesses, even in the absence of a Bureau rulemaking, represents a significant victory for innovation and for consumer and small business financial empowerment. The CFDR and FDATA North America both respectfully echo the Department's call for further action on this score by the BCFP.

2. *All regulators…should recognize the benefits of consumer access to financial account and transaction data in electronic form and consider what measures, if any, may be needed to facilitate such access for entities under their jurisdiction.*

One of the systemic disadvantages facing the fintech ecosystem in the United States as compared with many other countries that have imposed standards with regard to consumer-permissioned data access is the immense relative regulatory fragmentation that exists in the U.S. financial system. In the United Kingdom, for example, two agencies, the Financial Conduct Authority and the Competition and Markets Authority, represent the totality of regulatory authorities that were required to implement an entirely new, innovative approach to harnessing fintech under Open Banking. Mexico's CNBV and the Bank of Mexico are themselves responsible for developing and imposing financial API standards. The Australian Treasury and the Competition and Consumer Commission alone will deliver Open Banking in 2019.

There are at least eight federal regulatory agencies with jurisdiction over at least some portion of financial data access in the United States: the BCFP, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Federal Reserve Board of Governors, the Securities and Exchange Commission, the Commodity Futures Trading Commission, and the Federal Trade Commission. (Other federal agencies, including the Financial Crimes and Enforcement Network and the Financial Industry Regulatory Authority, have also been involved in the issue of consumer-

[15] *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation*. (2018, July 31). Retrieved from https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf

permissioned data recently.[16]) One commonly discussed regulatory constraint to the open transmission of permissioned consumer and small business financial data has been the prudential bank regulatory agencies' third-party vendor risk management guidance.[17]

There are also, of course, regulatory authorities in each state that have jurisdiction over entities that play a role in the fintech market, financial services providers and fintech firms alike. While Treasury cannot address the intrinsic, structural disadvantages in the United States' regulatory regime as compared with other countries', its call for all of the agencies in this space to align behind the Department's interpretation of Section 1033 of the Dodd-Frank Act is an important step towards a level playing field, and one that could be hastened by Congressional engagement. While, interestingly, some U.S. regulatory agencies have begun to collaborate with their peers internationally[18], greater domestic coordination that provides harmonization, rather than divergence, would spur innovation and improved consumer and small business financial outcomes.

3. *The Bureau [should] work with the private sector to develop best practices on disclosures and terms and conditions regarding consumers' use of products and services powered by consumer financial account and transaction data provided by data aggregators and financial services companies.*

The CFDR Group and FDATA North America strongly believe that consumers and small businesses should be empowered to use their financial data for their own financial benefit. To fully realize this empowerment, however, end users must be able to clearly and easily understand to what data elements they are granting third parties access to and for what purpose, as well as how they can revoke their consent to access and use the data. Though several industry groups have previously sought to establish guidelines in this space — and others continue to seek to formulate best practices — given the vast scope of the financial services market, very little standardization has taken place.

Fortunately, to the extent that the private sector, the BCFP and other regulatory agencies come together to develop best practices that could be adopted broadly across the industry, a market-tested framework already exists. The United Kingdom's Open Banking architecture includes prescriptive consent flows that ensure that a consumer's or small business' experience granting or revoking consent to access their data to any third party in the Open Banking environment is uniform. Accordingly, consumers in the Open Banking ecosystem experience the same consent-granting process across every third-party application they use, regardless of the financial institution with which they have their primary banking relationship. Offboarding is similarly uniform. The evidence suggests that end users of the Open Banking ecosystem are quickly becoming comfortable and familiar with these standards; three million Open Banking

---

[16] Know Before You Share: Be Mindful of Data Aggregation Risks. (2018, March 29). Retrieved from http://www.finra.org/investors/alerts/know-you-share-be-mindful-data-aggregation-risks

[17] Third-Party Relationships. (2017, June 7). Retrieved from https://www.occ.gov/news-issuances/bulletins/2017/bulletin-2017-21.html.

[18] BCFPB Collaborates with Regulators Around the World to Create Global Financial Innovation Network. (2018, August 7). Retrieved from https://www.consumerfinance.gov/about-us/newsroom/bcfp-collaborates-regulators-around-world-create-global-financial-innovation-network/

API calls were made this July, a month-over-month increase of 50 percent.[19] Public and private sector participants would do well to use these Open Banking consent standards as a starting point for creating best practices in the U.S. market.

4. *Any potential solution [to move to more secure and efficient methods of data access should] address resolution of liability for data access. If necessary, Congress and financial regulators should evaluate whether federal standards are appropriate to address these issues.*

The CFDR and FDATA North America believe that the issue of liability is the fundamental obstacle preventing the U.S. market from offering a more even, consumer-centric delivery of third-party tools powered by permissioned data connectivity. Decades-old regulations, such as Regulation E, create either the regulatory expectation or the consumer perception that financial institutions will largely make their customers whole in the event of any financial loss, including as a result of a data breach at a third party.[20] Further, prudential bank regulators have told the fintech community that the potential liability exposure to customers that nationally regulated banks face in the event of a data breach for which customers experience a financial loss represents a safety and soundness concern.

Largely as a result, some of the financial institutions seeking bilateral agreements with data aggregators are seeking to place the aggregator in the position of holding full, unlimited liability for the fintech ecosystem. These financial institutions hold that, because the aggregator is the only party with which they will have a bilateral agreement, the aggregator is the only entity from which they can recoup customer losses; however, this position is both impractical and untenable. Aggregators typically have no direct relationship with consumers or small businesses. Practically, they do not have the scale necessary to be in a position to provide their financial institution counterparties with boundless liability protection for the entire fintech market, nor would that fairly apportion responsibility throughout the ecosystem. As responsible stewards of consumer data, however, aggregators are prepared to be liable for any direct consumer harm that arises as a result of a breach for which they are at fault.

More broadly, the question of liability must also address the responsibility of the third party with which the consumer or small business has a relationship, whether it is a fintech application or a technology tool delivered by a traditional financial institution. The CFDR earlier this year released a set of principles, Secure Open Data Access ("SODA"), which called for the implementation of traceability, minimum cyber liability insurance standards and other standards designed to ensure that the entity responsible for consumer financial loss as a result of a data breach — be it a bank, an aggregator, or a fintech firm — is the entity charged with making the end user whole. While CFDR members are starting to implement the SODA principles with regard to liability, the financial regulatory agencies and Treasury could augment and assist this work by undertaking efforts to create a more vibrant and affordable cyber liability insurance market, similar to the steps taken by Her Majesty's Treasury in the United Kingdom last year.

---

[19] Open Banking Progress Update 13 July - 31 August. (2018, September 3). Retrieved from https://www.openbanking.org.uk/about-us/news/open-banking-progress-update-july-august-2018/

[20] 12 CFR 205

5. *Any potential solution [to move to more secure and efficient methods of data access should] also address the standardization of data elements as part of improving consumers' access to their data.*

Treasury notes in its report that "a standardized set of data elements and formats would help to foster innovation in services and products that use financial account and transaction data…"[21] While the CFDR Group and FDATA North America wholeheartedly agree with the Department's recommendation, I would respectfully submit an addendum to this recommendation. Standardization of data elements will only be impactful to American consumers and small businesses if they are able to grant access to all of the data required to power the use case they have selected. A standardized data set that, for example, does not allow end users to grant access to any data fields related to the fees or interest rates a financial institution assesses inherently restricts the ability of that customer to utilize fee comparison tools or to use a third-party tool to select an alternative, lower-cost provider.

Therefore, with the appropriate consent, authentication and liability safeguards in place, the standardized data elements made available to the consumer or small business to permit access to third parties of their choosing should include all of the data elements available to the end user in their native online banking environment. This approach would fully enable end users to leverage their own financial data to their economic benefit and it would allow for the realization of a competitive, free marketplace in which consumers have full transparency into financial products and services offered by fintech providers and financial services firms alike.

Conclusion

Though tens of millions of American consumers and small businesses are already utilizing third-party tools to improve their financial well-being, more can and should be done to harness the power of innovation and to give Americans full control of their own financial data and future. The Treasury's report provides an insightful overview of the outstanding issues facing the U.S. market that should be collaboratively addressed in order to better serve consumers and to ensure that the United States remains globally competitive as multiple countries implement comprehensive, consumer-centric financial data access frameworks. The CFDR Group and FDATA North America stand ready to work with the Department, the regulatory agencies, market stakeholders, and, of course, Congress, to implement the Treasury's recommendations.

[21] *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation*. (2018, July 31). Retrieved from https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf