February 21, 2017

Monica Jackson  
Office of the Executive Secretary  
Consumer Financial Protection Bureau  
1700 G Street NW.  
Washington, DC 20552

Re: CFPB-2016-0048 Request for Information Regarding Consumer Access to Financial Records

Dear Ms. Jackson,

The Center for Financial Services Innovation (CFSI) is submitting this letter in response to the request for information regarding consumer access to financial records, issued by the Consumer Financial Protection Bureau (CFPB) on November 17, 2016. Like you, we recognize the important role that access to high-quality financial products plays in helping consumers improve and maintain their financial health. We believe that finance can be a force for good in people’s lives and that meeting consumers’ needs responsibly is ultimately good for both the consumer and the provider.

CFSI is a national authority on consumer financial health. We believe that financial health comes about when a consumer’s day-to-day financial systems enable them to build resilience and pursue opportunities. We lead a network of financial services innovators – banks, the fintech community, processors, servicers, non-profits, and community-based organizations – all committed to building higher quality products and services. CFSI informs, advises and connects our network to seed innovation that will transform the financial services landscape. We hear the pain points and the see the opportunities from a variety of different viewpoints from both industry and consumers.

Through our consulting work, our Financial Capability Innovation Funds, and our Financial Solutions Lab, we have fostered innovative products and technologies that improve the financial health of consumers and nurture small businesses. Our vision is to see a strong, robust and competitive financial services marketplace, where the diversity of consumer transaction, savings and credit needs are met by a range of providers offering clear, transparent and high-quality products and services at reasonable prices.

CFSI recognizes that consumers’ ability to understand, manage and improve their financial health requires having a full picture of their financial lives. Today, as a result of technological advances and market developments, many of the products and services that provide consumers with this 360-degree view of their finances rely on data from numerous sources. There is a
critical need for industry collaboration to ensure that consumers have secure and reliable access to their financial data and to support continued innovation in the financial services marketplace.

In October 2016, CFSI released our Consumer Data Sharing Principles. These consumer-focused principles provide a framework to guide the industry as it works to establish a data-sharing ecosystem that is secure, inclusive and innovative. This effort builds upon CFSI’s previous work to establish principles and best practices guides for specific products, leveraging CFSI’s Compass Principles framework for quality in financial services. Specifically, we believe that an inclusive and secure financial data ecosystem is one in which financial institutions, data aggregators and third-party application providers coordinate to provide data to consumers that are:

- **Available**: Consumers have the ability to view their financial information within the trusted and secure third-party application of their choice (“Availability”).
- **Reliable**: Consumer financial data are timely, consistent, accurate and complete (“Reliability”).
- **User-permissioned**: Consumers provide explicit consent for access to and use of their data. Consumers can easily view, modify and revoke consent for data sharing (“Consent”).
- **Secure**: All entities follow applicable laws and industry best practices with regard to data privacy and security (“Security”).
- **Limited to the application functionality**: Only the minimum amount of data required for application functionality are collected, and the data are stored for the minimum amount of time needed (“Minimization”).

While these principles provide an important starting point, there is still significant work to be done to ensure they are applicable across the industry. Further coordination among all of the stakeholders in this debate – financial institutions, data aggregators, fintech providers, regulators and consumers themselves – will be critical to achieving a secure, inclusive and innovative financial data-sharing ecosystem that supports consumer financial health.

We believe that the CFPB has an important and constructive role to play in this process, and we applaud your effort to gather more information about current practices and potential market developments through this Request for Information.

In this letter, we provide some specific responses to some of the questions raised by the CFPB:

- Types of products and benefits to consumers of financial account aggregation
- Incentives and disincentives for financial account providers to facilitate access, and impacts for consumers
- Impediments, obstacles and risks for account providers, permissioned parties and consumers
- Potential market developments

We also share some other considerations about opportunities for the data sharing ecosystem and the role of the CFPB. In particular, we urge the CFPB to consider a principles-based approach to
this issue, avoiding the creation of specific rules that will soon become outdated with the quick pace of technological change and market developments. Finally, we offer some concluding remarks.

**Types of Products and Services and Benefits to Consumers (Question 1)**

In its Request for Information, the CFPB provided a detailed list of the various types of products and services that rely on consumer-permissioned electronic access to consumer financial account information. These include personal financial management tools, automatic and motivational savings, budgeting analysis and advice, product recommendations, account verification, loan application verification information, credit decisioning, cash flow management, funds transfer and bill payment, fraud and identity theft detection, and investment management and other non-consumer business services.

On the whole, these services provide consumers with greater visibility and control over their finances. In many cases, they enable the provision of real-time information, often via a mobile device, that help consumers to make better-informed decisions about spending, saving and borrowing. In other cases, they help consumers meet their savings or budgeting goals by leveraging automation and insights from behavioral economics. They can expand access to credit for underserved consumers by facilitating the evaluation of a broader set of data points (such as rent or utility reporting) for credit decisioning beyond just a formal credit score. They may also contribute to a more secure and efficient financial services system by enabling more streamlined processes for identity verification and fraud detection.

In CFSI’s [2016 FinLab Snapshot](#) report, we provide an overview of the number and types of companies that applied to be part of second class of the Financial Solutions Lab. Collectively, they provide a unique window into the state of consumer-focused financial technology in the United States. In 2016, 356 organizations responded to the call for applications, 19% more than in 2015. These applicants serve 4.2 million Americans, have raised over $420 million in external capital, and employ 2,293 people. They offer products focused on credit, insurance, investing, payments, planning, savings and other services that help consumer improve their financial health. Many of these innovative solutions rely on consumer-permissioned access to their users’ financial account information from multiple sources.

In our [FinLab Consumer Impact Report](#), we provide a look at the potential benefits that products that rely on consumer-permissioned access to financial account data have for their users. For example,

- **Digit** helps consumers automate savings by predicting their cash flow and identifying savings opportunities. Digit users have saved more than $350 million in less than two years of operation. On average, Digit users earn less than $40,000 per year and save more than 3% of their net income in their Digit account.

- **Even** helps consumers stabilize volatile income by guaranteeing a consistent amount of pay each pay period. During Q3 2016, Even users’ positive and negative swings in income averaged $175 in upswings and $125 in downswings. Regardless of how more or
less volatile a user’s income becomes over time, even guarantees their average take home pay each pay period.

- **Prism** makes bill pay easier by bringing all of a consumer’s bills together in an easy-to-use app. With all of their bills in one place, Prism enables consumers to make bill payments directly via ACH or with a credit, debit or prepaid card (65% of Prism users report having a bank account). As of November 2016, Prism has facilitated the bill payment of more than $50 million and saved thousands of customers from paying overdraft and late fees.

Consumers are clearly benefiting from a broader range of choices about the financial products and services they can use to manage their financial lives. Because many of the most effective tools in the market today rely on permissioned access to consumers’ financial information, ensuring secure and reliable access to these data is critical both for consumer choice and further innovation.

**Incentives and Disincentives for Financial Account Providers, and Impacts for Consumers (Question 8)**

In today’s digital world, financial account providers should have strong incentives to facilitate consumer-permissioned access to the account data they hold. Consumers have become accustomed to real-time access to their account information, and are increasingly turning to technology-enabled tools to help them manage their finances. Gone are the days of waiting 30 days for the next bank statement or keeping a shoebox full of receipts. For account providers seeking to foster customer loyalty and satisfaction, making it easy for their customers to grant permission to third parties to securely collect and use their financial information in ways that help customers meet their financial goals is simply smart business strategy.

It is important to remember that many financial institutions are not only providers of account-level information to third parties, but they are also beneficiaries of it. For example, many financial institutions rely on services provided by data aggregators to offer their customers financial management tools within their own bank-offered online or mobile interfaces. In addition, by facilitating access to account information, financial institutions can offer their customers a broader set of complementary products and services through partnerships with third parties. These strategies can help cement the account providers’ role as the center of the customer’s financial life, thereby increasing the longevity and long-term value of the relationship for both parties.

On the other hand, financial account providers might be disincentivized to facilitate access if they view permissioned third parties as potential competitors. However, CFSI believes that consumers have come to expect to be able to access and use their financial information in the application of their choice. Enabling access is no longer optional for financial account providers that wish to retain their customers’ loyalty. Yet, in order to be meaningful for consumers, that access must be provided in accordance with CFSI’s Data Sharing Principles, as described in further detail below.
Another issue for account providers is the ability of downstream actors to keep their customers’ data secure. Today, the predominant method of accessing data involves asking consumers for their bank login credentials, and using those credentials to “scrape” the data off of banks’ consumer-facing websites. There is currently a lack of clarity about which entity (or entities) would be liable in the event of a data breach in which a consumer’s account credentials were stolen from a third party and used to conduct fraudulent transactions. This lack of clarity, coupled with the fact that many financial institutions do not currently know which third parties are accessing their customers’ data, can be a disincentive for financial account providers to facilitate access.

Increasingly, the largest financial institutions are addressing these challenges and facilitating third-party access to their customers’ financial data in a variety of ways. Some are engaging in informal conversations with third parties to gather more information about them and their security practices, and “whitelisting” those who meet certain criteria – effectively granting approved third parties permission to access the data using consumers’ login credentials. Others are building the technical systems and risk management protocols to offer direct data feeds via Application Programming Interfaces (APIs) to approved partners, typically coupled with authentication technology that eliminates the need for consumers to share their login credentials.

Meanwhile, many smaller financial institutions are just beginning to become aware of this issue, and have not yet begun to proactively engage with third parties to facilitate access to the data they hold.

In CFSI’s Consumer Data Sharing Principles white paper, we emphasize the need for increased transparency and coordination among entities in order to achieve a data sharing environment that is secure, inclusive and innovative. We believe that the two approaches described above represent positive steps toward that goal, to the extent to which they contribute to greater trust among entities, and in doing so, facilitate the end consumer’s ability to access his or her data.

Impediments, obstacles and risks for account providers, permissioned parties and consumers (Questions 9, 10, 11)

As described in the previous section, there is risk to all parties (including consumers) due to the lack of certainty about where liability would fall in the event of a data breach. This is one reason why CFSI includes Security as one of our core principles for consumer data sharing, stating that “All entities [must] follow applicable laws and industry best practices with regard to data privacy and security.”

For account providers, particularly smaller financial institutions like community banks and credit unions, an additional obstacle is the investment required to build modern API infrastructure and negotiate data-sharing partnerships with third parties as a means to facilitate access. Small institutions do not have the resources to develop such technology or oversee a multitude of new third-party relationships, and typically rely on a third-party vendor for their core banking systems. Therefore, industry-wide collaboration will be needed to develop solutions that are inclusive of smaller institutions and their customers.
For permissioned parties, including data aggregators and consumer-facing applications, some of the most significant obstacles are disruptions in the flow of data, data that are unreliable, and high latency in the receipt of data from the account provider. In addition, the data available to third parties are sometimes not as up-to-date as the data the account provider can make available directly to the consumer. This limits a third party’s ability to provide a high-quality customer experience to its users, and may render the product itself less useful to the consumer.

For consumers, these same obstacles – disrupted connections, unreliable data and outdated information – can cause more harm than simply confusion and inconvenience. Because consumers often use these tools to help them make financial decisions, poor-quality data can actually cause them to take actions – such as paying a bill without sufficient funds in their checking account, thereby triggering an overdraft fee – that negatively impact their financial health. For these reasons, one of CFSI’s core Consumer Data Sharing Principles is the principle of Reliability: “Consumer financial data [must be] timely, consistent, accurate and complete.”

Another important principle is Control: “Consumers [must] provide explicit consent for access to and use of their data. Consumers [must be able to] easily view, modify and revoke consent for data sharing.” While consumer-facing application providers routinely ask consumers for consent to access data from financial institutions on their behalf, the ways in which those consent prompts and the corresponding terms of service disclosures are presented can vary significantly from application to application. Additionally, it may not always be clear to consumers how to view or modify previously-permissioned consent. The industry needs to work together to ensure that consumers are aware of, and actively consenting to, the opportunities and risks associated with sharing their financial data, and that they have ongoing agency to renew, revoke and change their consent.

**Market developments (Questions 18, 19, 20)**

In addition to the actions of account providers described above, we have recently seen the announcement of several bilateral partnerships between major financial institutions and large fintech providers to facilitate the transfer of consumer data through secure APIs.

As we stated earlier, CFSI sees such coordination among entities as a positive step forward, to the extent to which it facilitates the end consumer’s ability to access his or her data. However, to meet this expectation, such partnerships must be developed in line with CFSI’s Data Sharing Principles, particularly the principles of Availability and Reliability.

In order for new partnerships to meet the principle of Availability, which states that “consumers [must] have the ability to view their financial information within the trusted and secure third-party application of their choice,” there cannot be limits on the data fields that the financial account holder makes available to third parties with the consumer’s permission. A good rule of thumb may be that a consumer should have the ability to grant permission to a third party to access any piece of information that she would be able to see personally by logging into her account provider’s online portal.
As we noted earlier, data that are unreliable or out of date can have serious negative consequences for consumers who rely on that information to make financial decisions. Thus, in order to meet the principle of Reliability, data sharing partnerships between providers must also ensure that the data that are being transferred are always timely, consistent, accurate and complete.

Account providers have a significant interest in ensuring that the third parties accessing their systems are legitimate actors that have the technical and operational capacity to keep customer data safe. However, account providers must not attempt to use security concerns as a pretext for restricting access by imposing excessive requirements on third parties that will be impossible for all but the largest potential partners to accept. Similarly, account providers should not impose fees on consumer-permissioned third parties as a *de facto* method of restricting access to all but their most preferred partners.

There is likely a role for vetting and certification of trusted actors in the ecosystem. Data aggregators will have an important role to play as intermediaries between account providers and third-party applications, but one could also envision the creation of a new, independent body for certification. In either case, additional coordination across the industry to establish standards and best practices for vetting will help promote trust and transparency throughout the system and create a level playing field for future innovators.

### Other Considerations

**Principles vs. Rules and the Role of the CFPB**

CFSI believes the industry can come together develop standards and best practices for data sharing that enable consumer choice, are inclusive of smaller institutions and promote innovation. However, we think the CFPB has an important and constructive role to play by providing principles-based guidance that affirms consumers’ right to access their financial data. We believe that such guidance from the CFPB might be the catalyst that is needed to bring all of the necessary stakeholders to the table to develop effective industry-wide solutions. CFSI’s Data Sharing Principles may provide a useful starting place. However, we encourage the CFPB to avoid creating specific rules that, given the rapid pace of change in both technology and in the financial products and services these technologies enable, will quickly become antiquated and ultimately hamper innovation.

**Coordination with Other Regulators**

As described earlier, one of the obstacles that CFSI believes prevents more account providers from facilitating access to their customers’ data is the lack of clarity about the implications of existing regulations, such as those related to liability for consumer losses in the event of unauthorized transactions. We encourage the CFPB to coordinate with its counterparts in the OCC and other agencies to clarify how existing rules apply to third-party data access, where applicable, and to examine the ways in which principles-based guidance can help encourage more account providers to make their consumers’ data available to them in the third-party applications of their choice. In addition, given the increasingly important role that data
aggregators play as intermediaries and custodians of consumers’ data, we encourage the CFPB, OCC and other agencies to consider whether bringing them under more direct supervision would contribute to a more open and secure data sharing ecosystem.

**Role of Digital Identity**

In parallel to the current debate about financial data access, there are discussions taking place among industry and regulators about the role of digital identity technology in facilitating innovation in financial services. While these discussions are in their early days, there is significant potential for advances in digital identity technology to enable true consumer ownership and control of financial data. While the data access debate to date has focused primarily on accessing data from financial account providers, a next frontier for exploration could include the portability of data from one third-party provider to another – truly digitizing the proverbial shoebox of receipts. We encourage the CFPB to engage with its colleagues at the Treasury Department and other agencies as they evaluate the role of legal identity for financial inclusion, economic development and anti-money laundering/counter-financing of terrorism (AML/CFT) safeguards.

**Conclusion**

We appreciate the CFPB’s initiative in engaging with the industry and grappling with the issue of consumer-permissioned access to account data. We believe that consumers will be better able to achieve financial health if they have access to innovative products and services – many of which rely on access to such data to help their users manage their financial lives. Innovations can help consumers spend, save, borrow and plan safely and effectively, enabling them to manage their day-to-day finances, weather financial shocks, and providing them with longer-run financial opportunities.

We believe that the marketplace will benefit from a range of banks and fintech companies, start-ups and incumbents, and direct-service providers and partners all playing important roles in developing and delivering consumer-centric innovations. We recognize that regulators play an important role in keeping the market fair for both providers and consumers. We are glad that the CFPB is tackling the issue of how to ensure that consumers can access and control their financial data. We look forward to working with you as this effort moves ahead.

Sincerely,

Jennifer Tescher
President and CEO
Center for Financial Services Innovation

Beth Brockland
Managing Director
Center for Financial Services Innovation