Stuart Rubinstein
Head of Data Aggregation
President, Fidelity Wealth Technologies
245 Summer Street V7A
Boston, MA 02210

March 15, 2019

Submitted Electronically to submissions@banking.senate.gov

The Honorable Mike Crapo
Chairman
U.S. Senate Committee on Banking,
Housing, and Urban Affairs
534 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Sherrod Brown
Ranking Member
U.S. Senate Committee on Banking,
Housing, and Urban Affairs
534 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Crapo and Ranking Member Brown:

Introduction

In response to your February 13, 2019, invitation to provide feedback on data privacy, protection, and collection, Fidelity Investments ("Fidelity")[1] is pleased to provide recommendations to the U.S. Senate Committee on Banking, Housing, and Urban Affairs (the "Committee") on concrete ways to make consumer-directed sharing of financial data safer and more transparent for financial institutions, data aggregators, fintech firms, and—most importantly—consumers. We appreciated the opportunity to testify before this Committee on this topic last September[2] and commend your continued bipartisan leadership on these critical data protection issues.

Our response focuses on the policy challenges of financial data aggregation implicated in the first three questions of the Committee's request for feedback. As discussed below, Fidelity recommends that, as this Committee and other policymakers develop policies, they have a clear goal of protecting consumers' financial account data.[3]

Issues associated with financial data aggregation have received increasing attention from policymakers, the private sector, and consumers over the past several years. While this debate has increased awareness and facilitated discussion about the potential risks and harms of existing

[1] Fidelity is one of the world's largest providers of financial services, including investment management, retirement planning, portfolio guidance, brokerage, benefits outsourcing and many other financial products and services to more than 30 million individuals and institutions, as well as through 12,500 financial intermediary firms.

[2] *See Fintech: Examining Digitization, Data, and Technology: Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 115th Cong. (statement of Stuart Rubinstein, President, Fidelity Wealth Technologies & Head of Data Aggregation), *available at* https://www.banking.senate.gov/imo/media/doc/Rubinstein%20Testimony%209-18-18.pdf.

[3] By financial account data, we mean account level data (typically data such as balances, transactions, and holdings) that customers of a financial services firm may desire to have shared with the data aggregator in order to perform a specific service for the customer.

financial data aggregation practices, in addition to the benefits to consumers, we believe there has been an insufficient sense of urgency for adopting more secure data sharing practices. Accordingly, we recommend the Committee and other policymakers provide the marketplace with clear direction on how best to protect consumers' financial data.

Current State of Financial Data Aggregation

As we noted in our testimony before this Committee, Fidelity has a unique perspective on data aggregation: we are an aggregator of financial data for third parties; we are a significant source of data for financial data aggregators acting on behalf of our mutual customers; and we offer a financial data aggregation service for our retail customers and retirement plan participants. As such, we understand the current financial data aggregation ecosystem—both the benefits for consumers and the very real cyber and data security risks.

Financial data aggregation in this context refers to services that, at a customer's direction and with the customer's permission, collect financial account information from the customer's various bank, brokerage, and retirement accounts, along with other sources, to be displayed and processed in an aggregated view for the customer. Consumers use third party applications that leverage financial data aggregation because they value tools to help manage their financial planning, budgeting, tax preparation, and other needs. Customers have been able to use their financial account data from Fidelity in third party applications for many years; however, the cybersecurity environment has become more perilous over that time, and we as a financial services firm have a responsibility to protect the personal financial account data and assets that we maintain for our more than 30 million customers.

Current financial data aggregation practices make this challenging, because they rely on consumers providing their financial institution log-in credentials (*i.e.*, username and password) to third parties. Those third parties, typically data aggregators, then almost always employ a practice known as "screen scraping." At its most basic element, screen scraping involves the use of computerized software "bots" to log-in to financial institution websites, mobile apps, or other applications utilizing the consumers' log-in credentials as if they were the consumer. Once the bots have access to a site or app, they copy—or "scrape"— data about the consumers' accounts from the various screens. The data is collected and stored by the data aggregator to be presented to the consumer on a consolidated basis, along with information scraped and collected from other sources. While some of those companies who employ this process have made progress in moving to safer sharing technologies by adopting, for example, application programming interfaces (APIs),[4] the vast majority of financial data aggregation participants use the outdated and risky screen scraping model.

[4] An API works in conjunction with an authentication process that is handled by the financial institution. The authentication process, called "open authorization" ("OAuth"), does not involve sharing of account access credentials with aggregation services. Consumers who want their data aggregated are directed by the aggregation service to provide their account credentials directly with their financial institution (through a webpage provided by the firm). At that time, the consumer can be provided with a consent screen to provide authorization to the financial services firm to make data accessible to the aggregation service.

Fidelity believes that, as a fundamental security protection, consumers should not be asked for or required to share their personal and private financial institution log-in credentials with a third party service in order for the consumer to share their financial account data with that service. While this statement should appear self-evident, there are some who offer financial data aggregation services that would continue this practice. Allowing third parties to log-in with customer credentials creates significant security risks, including risks to cybersecurity, data security, and identity theft. Because in most cases consumers go directly to data aggregators or their commercial clients[5] and not their financial institution, the financial institutions may not know if the activity has in fact been authorized by the customers.

We believe this status quo is unacceptable, and without action by Congress there is unlikely to be a significant shift to safer practices in any reasonable amount of time.

Recent Policymaker Action

The cybersecurity environment is changing significantly, and as financial firms have adapted they began to raise concerns about current financial data aggregations practices.[6] Correspondingly, regulators have appropriately focused heightened concern on policy implications of financial data aggregation, looking for ways to foster innovation without sacrificing critical investor and consumer protection safeguards. This interest has been enormously helpful in clarifying the scope of the issues.

In 2016, the Bureau of Consumer Financial Protection (CFPB) issued a request for information (RFI) inviting comment on financial data sharing practices that the next year culminated in helpful principles to guide aggregators and financial firms.[7] These principles note the need for access, security, transparency, and informed consent. Fidelity provided comments and feedback to the CFPB during its information gathering process and believes the principles are a helpful framework.[8]

In March 2018, the Financial Industry Regulatory Authority (FINRA) published a helpful investor alert reviewing the risks to investors of using aggregation-based services and observing that many industry participants were moving to safer technologies, like application programming interfaces (APIs). Fidelity has regularly engaged with FINRA on this issue, including providing

[5] An example of a commercial client of an aggregator might be an investment advisor or other financial institution that has hired the aggregator for data aggregation services.

[6] Securities Industry and Financial Markets Association (SIFMA), *Data Aggregation Principles* (2018), https://www.sifma.org/wp-content/uploads/2018/04/sifma-Data-Aggregation-Principles.pdf.

[7] Bureau of Consumer Financial Protection (CFPB), *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* (October 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

[8] *See* Requests for Information: Consumer Access to Financial Records, 81 Fed. Reg. 83806 (posted Nov. 17. 2016)(comments of Stuart Rubinstein, Fidelity Investments), *available at* https://www.regulations.gov/document?D=CFPB-2016-0048-0053.

feedback on its recent request for comment on Financial Technology in the broker-dealer industry.[9]

Most recently, the Department of the Treasury released a report on Nonbank Financials, Fintech, and Innovation that includes a lengthy discussion of data aggregation technologies, as well as the significant cybersecurity, data security, and innovation policy implications of current industry practices. While the report does not recommend additional regulation it does recommend the industry adopt simplified disclosures, move away from screen scraping, and end the practice of credential sharing.

Congress is appropriately focused on data privacy concerns, including the challenges involved with the sharing and aggregation of financial account data. We are encouraged that Members are focused on these important issues. Fidelity welcomed the opportunity to further the public discourse on the topic by testifying before this Committee and the House Financial Services Committee Subcommittee on Financial Institutions and Consumer Credit outlining our views on financial data aggregation.[10]

While recent attention to financial data aggregation practices has raised awareness for consumers and policymakers, the industry is not moving quickly away from harmful and risky data sharing practices despite the availability of safer technologies.

Fidelity's Views on How to Best Protect Consumers

As Fidelity has used its unique position in the market to listen to stakeholders on all sides of this issue, we have developed a set of principles that should guide policymakers and the private sector in evaluating potential safer financial data sharing technologies. We presented these five principles to the Committee in September, but reiterate them here:

- **We strongly support consumers' right to access their financial account data and provide that data to third parties**. As a provider of aggregation services ourselves, we know that customers value these services, and the demand for aggregation of financial account data is likely to increase. We also believe that the concept of access is broad enough to encompass security, transparency, and cybersecurity protections for consumers.

- **Data access and sharing must be done in a safe, secure, and transparent manner**. We firmly believe credential sharing makes the system less safe for consumers, aggregators, and financial institutions alike. While we strongly support customer access

[9] *See* FINRA Requests Comment on Financial Technology Innovation in the Broker-Dealer Industry (posted July 30, 2018)(comments of Fidelity Investments), http://www.finra.org/sites/default/files/SPNotice-7-30_fidelity_comments.pdf.

[10] *See Examining Opportunities for Financial Markets in the Digital Era: Hearing Before the H. Financial Services Comm. Subcomm. on Financial Institutions and Consumer Credit*, 115th Cong. (statement of Stuart Rubinstein, President, Fidelity Wealth Technologies & Head of Data Aggregation), *available at* https://republicans-financialservices.house.gov/uploadedfiles/hhrg-115-ba15-wstate-srubenstein-20180928.pdf

to their financial account data, the security of that data, customer assets, and financial institution systems must be our primary concern.

- **Consumers should provide affirmative direction and instruction to financial institutions to share their data with third parties**. Rather than require that financial institutions trust that third parties who use customer log-in credentials to access the financial institution's website are authorized by that customer, customers should tell financial institutions which third parties have permission to access their financial account data. This eliminates the potential that unauthorized access using credentials is mistaken for authorized access.

- **Third parties should access the minimum amount of financial account data they need to provide the service for which the customer provided access**. There should be a tight nexus between the service provided and the information collected by third party aggregators. For example, if a customer signs up for a tax planning service that leverages aggregation, that service should only access the information needed for tax planning.

- **Consumers should be able to monitor who has access to their data, and access should be easily revocable by the consumer**. We believe data sharing and permissioning should be an iterative process, with customers engaged continuously. Moreover, many customers believe revoking access is as easy as deleting an app from their phone—this is not the case. Customers should be able to easily instruct their financial institution to revoke access when they no longer want or need the aggregation-based service.

Despite consensus that the status quo is unacceptable and agreement that some formulation of the above principles constitute a workable, safer data sharing ecosystem, there are roadblocks preventing wider adoption of safer data sharing technologies. These challenges include: (1) getting firms to adopt new technologies where existing practices have been the norm for decades; (2) the cost incurred in moving to safer technologies like APIs; and (3) challenges surrounding apportioning liability, specifically with third party aggregators who want to limit their potential exposure in the event that financial data is illicitly obtained from them. Fidelity believes firms that obtain and handle data for their customers should assume full responsibility to protect that data from loss or unauthorized access or use.

A Call to Action to Improve Financial Data Aggregation

As noted at the outset of these comments, given the critical cyber and data security interests at stake for consumers and financial institutions alike, financial firms, aggregators, and fintech firms should be swiftly moving to safer data sharing technologies. Accordingly, we recommend to this Committee the following consumer and investor protection focused policy changes for your consideration:

- **Consumers' right to access and share financial account data**: Consumers have the right to access their personal financial account data and direct a financial institution to allow third parties specified by the consumer to access their data. Congress should create

consumer protection principles governing how financial institutions, aggregators, and fintech firms share consumers' financial account data.

- **Minimum consumer protection standards for data sharing**: While consumers have a right to access their financial account data and grant access to that data to third parties, that sharing must be done pursuant to minimum standards of security and transparency. Third parties that wish to receive financial account data should be required to show that they maintain a baseline level of security standards. Financial institutions must have the ability to protect their own systems from dangerous practices. A policy solution should not mandate a specific technology, but should require firms to adopt newer, safer technologies when they become available and scalable.

- **Affirmative direction by consumer**: Consumer-directed access and sharing of financial account data should only be done pursuant to the affirmative direction and permission given by the consumer directly to the financial institution holding the consumer's data. Financial institutions should be required to record this direction and permission. Third parties using a consumer's log-in credentials to access a financial institution's website should not qualify as implied direction or permission.

- **Access and sharing for a specific purpose**: When consumers direct financial institutions to permit third parties to access their financial account data, they do so for a single third party and for a specific use case—i.e., wealth planning, personal budgeting, etc. Financial institutions should only share the data fields necessary to provide the requested service to the consumer, and third parties should use the data only for those purposes. Any use of the data by a third party for other purposes should require that third party obtain consent from the consumer for each additional use case.

- **Continuous monitoring by consumer**: Financial institutions should provide consumers with the ability to monitor which third parties the customer has allowed to access their financial account data and for what purpose(s) the third party is using that data.

- **Ability to revoke**: Consumers should also be able to easily instruct their financial institution to revoke specific or all third party access to their financial account data that was previously directed by the consumer.

- **Liability for consumer harm**: Acceptance of liability is the greatest roadblock for wider adoption of safer financial data sharing technology. Accountability and responsibility for addressing consumer harm must follow the data, should the data in possession of an aggregator or other third party be compromised. As a straightforward policy proposition: the party that causes a consumer harm must be responsible for making that consumer whole. Additionally, if a third party loses, misappropriates, or otherwise mishandles a consumer's data and that data is used to cause a loss to the consumer or the financial institution, the third party should be required to make the consumer or financial institution whole.

We believe these basic policies would facilitate a much safer financial data sharing and aggregation ecosystem for all parties—consumers, financial firms, aggregators, and fintech

firms. Moreover, there is significant consensus around these reforms. Congress should fulfill a leadership role and move quickly to introduce and advance legislation embodying these principles.

Conclusion

Nearly everyone agrees that the status quo for financial data aggregation is unacceptable, and the vast majority of industry participants agree about the basic tenets of a solution; however, we have not seen change with a sense of urgency commensurate with the risks. We still believe that industry can solve the majority of these problems, but we are having difficulty translating considered discussion into momentum. Indeed, Fidelity is working hard to facilitate safer financial account data sharing and aggregation technologies. However, the time has come for Congress to provide leadership. We must make the consumer-directed sharing of financial data safer and more transparent for financial institutions, data aggregators, fintech firms, and—most importantly—the American consumer.

We would be happy to provide the Committee with additional information, perspective, or resources as you work through these critically important issues.

Sincerely,

Stuart Rubinstein
Head of Data Aggregation
President, Fidelity Wealth Technologies