Testimony of

Stuart Rubinstein
President, Fidelity Wealth Technologies & Head of Data Aggregation

Before the

U.S. Senate Committee on Banking, Housing, and Urban Affairs

Hearing entitled
"Fintech: Examining Digitization, Data, and Technology"

September 18, 2018

Chairman Crapo, Ranking Member Brown, and Members of the committee: thank you for holding this important hearing. Fidelity is very interested in fintech and data policy and has a unique perspective to share on financial data account access and aggregation used by many fintech firms.

My name is Stuart Rubinstein and I am President of Fidelity Wealth Technologies and Head of Data Aggregation. In this role, I oversee the team focused on helping Fidelity and other institutions enable consumers to securely share account data and documents with third parties. Fidelity is a leading provider of investment management, retirement planning, portfolio guidance, brokerage, benefits outsourcing, and other financial products and services to more than 30 million individuals, institutions, and financial intermediaries with more than $7 trillion in assets under administration. Our goal is to make financial expertise broadly accessible and effective in helping people live the lives they want.

I will focus my testimony for this hearing on an issue I first worked on over 20 years ago: financial data aggregation services and ways we can make data sharing safer and more secure.

Fidelity's Perspective on Data Aggregation

Fidelity has a unique perspective on financial data aggregation practices and necessary protections for customers. We are on all sides of this issue: we are an aggregator of data for third parties,[1] we are a significant source of data for aggregators acting on behalf of our mutual customers, and we offer a data aggregation service for our retail customers and retirement plan participants.[2] This perspective gives us a thorough understanding of the benefits of financial data aggregation, but also of the very real cybersecurity and privacy risks that current data aggregation industry practices create.

Financial data aggregation in this context refers to services that, with customers' consent, collect financial information from their various bank, brokerage, and retirement accounts, along with other sources, to be displayed and processed in an aggregated view. An example of this kind of service might be a budgeting and planning smartphone app. Consumers use third party applications that leverage data aggregation because they value tools to help manage financial planning, budgeting, tax preparation, and other services. As part of our focus on helping our customers, Fidelity works to make it possible for customers to access the services they want to use—including third party aggregation-based services. To that end, customers have been able to use their Fidelity data in third party applications for many years. However, the cybersecurity environment has significantly changed over that time and we have a responsibility to protect the very sensitive personal financial data and assets of our more than 30 million customers from misuse, theft, and fraud.

[1] Financial advisors can use *eMoney Advisor*, a Fidelity-owned business that provides account aggregation services along with software that helps them provide financial advice to their clients.

[2] Fidelity offers its *FullView*® services to retail customers through Fidelity.com and to retirement plan participants through NetBenefits.com, and developed its first account aggregation service over fifteen years ago. Fidelity *FullView* provides a snapshot of customers' net worth in a simple format with an ability to do budgeting and financial planning.

Current 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, screen scraping involves the use of computerized "bots" to log-in to financial institution websites, mobile apps, or other applications as if they were the consumer. Once the bots have access to the site or app, they "scrape" customer data from the various screens to be presented on a consolidated basis, along with information scraped and collected from other sources.

There are two consumer data security problems with this practice. First, as a matter of basic security consumers should not be asked or required to share their private log-in credentials in order to access a third party service. Doing so creates cybersecurity, identity theft, and data security risks for the consumer and financial institutions. Unfortunately, we know that due to years of this practice, financial institution log-in credentials are now held by a myriad of companies. Some are likely very secure, while others may not be secure at all. Given this, allowing third parties to log-in using these credentials as if they are the customer creates significant risk of cyber-fraud. Because consumers go directly to data aggregators or their commercial clients and not their financial institution, the financial institutions never really know if the activity has in fact been authorized by the customers or if the customer credential has been compromised and a criminal is using the data aggregation service to test the credential's validity and illicitly gather data.

Second, screen scraping may result in access to data fields far beyond the scope of the service a third party offers the consumer—including personally identifiable information (PII) about consumers and in some cases their dependents. This means third parties have access to fields of information often used by financial institution call centers to identify customers. For example, if a consumer provides his or her log-in credentials to a budgeting app, that app potentially has access to sensitive personal information like customer dates of birth and dependent names and dates of birth, all of which might be data financial institutions use to verify customer identities online or over the phone. Collection of information beyond what is needed for the service the consumer has elected creates unnecessary risk. And all of this adds up to an array of risks financial institutions must navigate to protect the integrity of their systems and the assets of their customers.

In considering the challenges described above, Fidelity developed the following five principles that we believe should guide industry in creating better data sharing solutions:

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

2. **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,

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

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

4. **Third parties should access the minimum amount of financial 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.

5. **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.

We believe that embracing these principles will better protect consumers, aggregators, and financial institutions, and facilitate more efficient data sharing practices.

How Do We Solve This for Consumers?

Fortunately, although the risks and challenges of the current system are serious, there are steps financial institutions and aggregators can take together to improve the data sharing ecosystem. The financial services industry is employing technological solutions for the secure exchange and access of financial information. These technologies involve the implementation and use of application programming interfaces ("APIs"), which are provided by the financial institution to aggregators and other third parties. An API works in conjunction with an authentication process that is handled by the financial institution. There are authentication processes, for example "open authorization" ("OAuth"), that do not involve sharing of account access credentials with third parties. Consumers who want their data aggregated sign into their accounts at the financial institution's website and provide authorization for third party aggregators to access their financial data. The financial institution and the data aggregator then manage that connection through secure, encrypted tokens that are provisioned for the specific connection.

There are several compelling consumer and data security benefits for moving to APIs. First, it keeps log-in credentials private and secure by eliminating the need for consumers to share log-in credentials with third parties. This reduces the cyber, identity, and personal data security risks that exist when a consumer shares private log-in details with a third-party. Second, it puts the consumer in the driver's seat by giving consumers greater transparency and control of their data

by allowing consumers to provide unequivocal consent and instruction to share their data with third parties. Third, it allows financial institutions and aggregators to agree on what data should be shared and avoid over-scraping. Fourth, it eliminates the need to reconfigure aggregators' systems every time a consumer changes his or her username or password or the financial institution updates its webpage. Fifth, it removes the traffic-intensive screen scraping activity from financial institutions' web sites and other digital properties, returning that capacity to the individual consumers for whom those sites were created. Finally, it enables the consumer to monitor the ongoing access and instruct their financial institution to revoke the consent if desired.

Fidelity Access

In November 2017, Fidelity announced its own API solution for data sharing called *Fidelity Access*SM. *Fidelity Access* will allow Fidelity customers to provide third parties access to customer data through a secure connection without providing log-in credentials. *Fidelity Access* will include a control center, where customers can grant, monitor, and revoke account access at any time. We have been working closely with aggregators and other third parties on adoption of this solution.

Of particular note, *eMoney Advisor*, Fidelity's affiliate that offers its own aggregation service, is committed to working with other financial institutions that offer APIs. By championing the exclusive use of APIs to facilitate customers providing third parties access to their financial data, we hope to show leadership by taking action to better secure our customers' data.

Industry Standards and Policymaker Guidance

In addition to our own efforts to address the problems with data aggregation, we have been working with a wide array of industry and public sector stakeholders. We support many of the data sharing and aggregation principles that have been put forth:

- In October 2017, after a year-long inquiry into the topic, the Bureau of Consumer Financial Protection (BCFP) released non-binding financial data sharing and aggregation principles, which helpfully emphasized the importance of access, security, transparency, and consent.[3]

- In February 2018, the Financial Services Information Sharing and Analysis Center (FS-ISAC), a cybersecurity information sharing group focused on the financial services industry, published a standard durable data API free of charge to help facilitate safer transfer of financial data.[4] The Fidelity Access API is based on this standard.

[3] *Available at* https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf. Fidelity commented on the Request for Information that culminated in these principles (https://www.regulations.gov/document?D=CFPB-2016-0048-0053).

[4] *See* https://www.fsisac.com/article/fs-isac-enables-safer-financial-data-sharing-api. Fidelity is a member of FS-ISAC and contributed to the development of the durable data API.

- In March 2018, the Financial Industry Regulatory Authority (FINRA) published an investor alert that explained the risks associated with aggregation-based services and noted that many firms are moving toward APIs.[5]

- In April 2018, the Securities Industry and Financial Markets Association (SIFMA) released data aggregation principles that focused on similar themes.[6]

- In July 2018, the U.S. Department of the Treasury released a report on Nonbank Financials, Fintech, and Innovation that includes a lengthy discussion of financial data aggregation and helpful recommendations, including simplified disclosures, moving away from screen scraping, and eliminating log-in credential sharing.[7]

These efforts to provide guidance have brought many of the challenges and risks associated with data aggregation to the fore and encouraged healthy debate on how to solve them.

Continuing Challenges

Despite the general consensus that the status quo is untenable and the industry should move to safer data sharing technologies, there are roadblocks that prevent wider adoption of APIs and other solutions. Here are what we see as the most challenging:

- Inertia: One force working against adoption of safer data sharing technologies is simple inertia. Existing practices have been the norm for close to two decades. Getting firms to adopt new technologies can be challenging no matter what the benefits. However, given the stakes, with headlines replete with examples of cybersecurity events and data breaches, this is not an adequate reason to resist better data sharing technology.

- Cost: Another countervailing force is cost. One of the unfortunate truths about screen scraping is that it is cheap and effective. While safer technologies like APIs have become less costly as technology advances, building one does incur costs. We believe the incremental increase in cost is well worth the substantial security and transparency improvements for consumers. Still, financial institutions should be sensitive to this reality, which is why we are providing *Fidelity Access* to third parties free of charge.

- Liability: Liability is the most stubborn blocker to wider adoption of safer data sharing technologies. Third party aggregators want to limit their potential liability in the event that financial data is illicitly obtained. We have seen firms try to limit their liability to low dollar amounts. These kinds of limits are untenable for financial firms like Fidelity that have a duty to protect client assets. Fidelity believes firms that obtain and handle consumer data should be held responsible to protect that data from unauthorized use, just

[5] *Available at* http://www.finra.org/investors/alerts/know-you-share-be-mindful-data-aggregation-risks.
[6] *Available at* https://www.sifma.org/resources/general/data-aggregation-principles/. Fidelity is a member of SIFMA and worked closely with other member firms in developing these principles.
[7] *Available at* https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf.

as we are. Any other standard creates moral hazard and does not incentivize aggregators to take their data stewardship responsibilities seriously.

Until all industry participants—aggregators, fintech firms, and financial institutions—are prepared to overcome these challenges in a responsible manner, we will not move as swiftly as we otherwise could to adopt safer data sharing technologies.

* * *

Thank you again for the opportunity to testify and I look forward to answering your questions.

859441.1.0