

BANKING ON YOUR DATA: THE ROLE OF BIG DATA IN FINANCIAL SERVICES

HEARING BEFORE THE TASK FORCE ON FINANCIAL TECHNOLOGY OF THE COMMITTEE ON FINANCIAL SERVICES U.S. HOUSE OF REPRESENTATIVES ONE HUNDRED SIXTEENTH CONGRESS FIRST SESSION

NOVEMBER 21, 2019

Printed for the use of the Committee on Financial Services

Serial No. 116-69



U.S. GOVERNMENT PUBLISHING OFFICE

42-477 PDF

WASHINGTON : 2020

HOUSE COMMITTEE ON FINANCIAL SERVICES

MAXINE WATERS, California, *Chairwoman*

CAROLYN B. MALONEY, New York	PATRICK McHENRY, North Carolina,
NYDIA M. VELAZQUEZ, New York	<i>Ranking Member</i>
BRAD SHERMAN, California	ANN WAGNER, Missouri
GREGORY W. MEEKS, New York	PETER T. KING, New York
WM. LACY CLAY, Missouri	FRANK D. LUCAS, Oklahoma
DAVID SCOTT, Georgia	BILL POSEY, Florida
AL GREEN, Texas	BLAINE LUETKEMEYER, Missouri
EMANUEL CLEAVER, Missouri	BILL HUIZENGA, Michigan
ED PERLMUTTER, Colorado	STEVE STIVERS, Ohio
JIM A. HIMES, Connecticut	ANDY BARR, Kentucky
BILL FOSTER, Illinois	SCOTT TIPTON, Colorado
JOYCE BEATTY, Ohio	ROGER WILLIAMS, Texas
DENNY HECK, Washington	FRENCH HILL, Arkansas
JUAN VARGAS, California	TOM EMMER, Minnesota
JOSH GOTTHEIMER, New Jersey	LEE M. ZELDIN, New York
VICENTE GONZALEZ, Texas	BARRY LOUDERMILK, Georgia
AL LAWSON, Florida	ALEXANDER X. MOONEY, West Virginia
MICHAEL SAN NICOLAS, Guam	WARREN DAVIDSON, Ohio
RASHIDA TLAIB, Michigan	TED BUDD, North Carolina
KATIE PORTER, California	DAVID KUSTOFF, Tennessee
CINDY AXNE, Iowa	TREY HOLLINGSWORTH, Indiana
SEAN CASTEN, Illinois	ANTHONY GONZALEZ, Ohio
AYANNA PRESSLEY, Massachusetts	JOHN ROSE, Tennessee
BEN McADAMS, Utah	BRYAN STEIL, Wisconsin
ALEXANDRIA OCASIO-CORTEZ, New York	LANCE GOODEN, Texas
JENNIFER WEXTON, Virginia	DENVER RIGGLEMAN, Virginia
STEPHEN F. LYNCH, Massachusetts	WILLIAM TIMMONS, South Carolina
TULSI GABBARD, Hawaii	
ALMA ADAMS, North Carolina	
MADELEINE DEAN, Pennsylvania	
JESUS "CHUY" GARCIA, Illinois	
SYLVIA GARCIA, Texas	
DEAN PHILLIPS, Minnesota	

CHARLA OUERTATANI, *Staff Director*

TASK FORCE ON FINANCIAL TECHNOLOGY

STEPHEN F. LYNCH, Massachusetts, *Chairman*

DAVID SCOTT, Georgia
JOSH GOTTHEIMER, New Jersey
AL LAWSON, Florida
CINDY AXNE, Iowa
BEN McADAMS, Utah
JENNIFER WEXTON, Virginia

TOM EMMER, Minnesota, *Ranking Member*
BLAINE LUETKEMEYER, Missouri
FRENCH HILL, Arkansas
WARREN DAVIDSON, Ohio
BRYAN STEIL, Wisconsin

CONTENTS

	Page
Hearing held on:	
November 21, 2019	1
Appendix:	
November 21, 2019	31

WITNESSES

THURSDAY, NOVEMBER 21, 2019

Cardinal, Don, Managing Director, Financial Data Exchange (FDX)	10
Gilliard, Christopher, Professor of English, Macomb Community College, and Digital Pedagogy Lab Advisor	8
Kamara, Seny, Associate Professor of Computer Science, Brown University, and Chief Scientist, Aroki Systems	6
Pozza, Duane, Partner, Wiley Rein	11
Saunders, Lauren, Associate Director, National Consumer Law Center (NCLC)	4

APPENDIX

Prepared statements:	
Cardinal, Don	32
Gilliard, Christopher	42
Kamara, Seny	48
Pozza, Duane	54
Saunders, Lauren	62

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Lynch, Hon. Stephen:	
Written statement of the American Bankers Association	83
Written statement of the Credit Union National Association	92
Written statement of the Electronic Transactions Association	94
Written statement of the Financial Data and Technology Association	96
Written statement of Fidelity Investments	99
Written statement of Finicity	106
Written statement of Plaid	115
Written statement of Public Knowledge	117
Hill, Hon. French:	
Written responses to questions submitted to Don Cardinal	122
McAdams, Hon. Ben:	
Written responses to questions submitted to Don Cardinal	124
Written responses to questions submitted to Duane Pozza	128
Written responses to questions submitted to Lauren Saunders	130

BANKING ON YOUR DATA: THE ROLE OF BIG DATA IN FINANCIAL SERVICES

Thursday, November 21, 2019

U.S. HOUSE OF REPRESENTATIVES,
TASK FORCE ON FINANCIAL TECHNOLOGY,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The task force met, pursuant to notice, at 9:30 a.m., in room 2128, Rayburn House Office Building, Hon. Stephen F. Lynch [chairman of the task force] presiding.

Members present: Representatives Lynch, Scott, Gottheimer, Lawson, Axne, McAdams; Emmer, Luetkemeyer, Hill, Davidson, and Steil.

Also present: Representatives Tlaib, Gonzalez of Ohio, and Hollingsworth.

Chairman LYNCH. Good morning. The Task Force on Financial Technology will now come to order.

Without objection, the Chair is authorized to declare a recess of the task force at any time. Also, without objection, members of the full Financial Services Committee who are not members of the task force are authorized to participate in today's hearing.

Today's hearing is entitled, "Banking on Your Data: The Role of Big Data in Financial Services."

Before we get started, I want to take a moment to recognize our new ranking member, Mr. Tom Emmer, from the great State of Minnesota. Welcome. Mr. Emmer has a keen interest in the fintech space and has been active in this area for some time, and I am looking forward to learning from and working with him going forward.

I also want to thank my friend and colleague, Mr. French Hill of Arkansas, who escaped this task force, and is now the ranking member on the National Security Subcommittee, which I Chair. I wish him the best of luck in that endeavor, and I am glad to still have his voice on this task force.

I now recognize myself for 4 minutes to give an opening statement.

In July, our task force examined the potential benefits and the risks associated with the use of alternative data in credit underwriting. We noted that the use of alternative data can expand access to credit for those who might otherwise be turned away from lenders. And we also discussed the possibility of that data being

linked to disparate impacts on the unfair credit decisions that might be made.

But in financial services, the use of data goes far beyond consumer or small business lending. The rise of financial and consumer data has enabled an explosion of financial products and services for consumers to use. Because of the volume and transferability of this data, consumers have access to applications to manage their finances, change their savings habits, or pay their friends in a way that wasn't possible a few years ago.

However, the prevalence of financial applications has led to more and more personal financial data being transmitted and held outside of the traditional financial system. While most companies want to protect their customers' data, this trend has caused many to question whether our existing statutory protections are indeed adequate for the new circumstances.

Consumers rightly expect their financial data to be kept secure by institutions and applications they use, but unfortunately, their expectations don't always match reality. Large-scale breaches of consumer data, like those at Equifax and Capital One, serve as a vivid reminder that even legacy institutions can be vulnerable to security lapses. They also remind us how painful it can be for a consumer to have their personal information stolen through no fault of their own.

As consumers use their financial data in more ways and in more places, it becomes increasingly difficult for them to know exactly how their data is being used and, making it worse, many applications come with lengthy terms-of-service agreements which are not conducive to being read on the mobile devices consumers are using to agree to them. So we all tend to just click, "I agree," without realizing the consequences.

According to recently released research by the Clearing House, 79 percent of users said they did not read all the terms and conditions, and only 11 percent said they both read and understood them. Most of those people are lying. Further, the technical aspects of data security are opaque and complex. This makes it even more important for Congress and our financial regulators to get this right.

The future of connected or open banking, the process of transmitting the data necessary to enable the success of these financial applications, depends on the industry's ability to do so in a safe and secure way. While there is undeniable potential in this space, today we will discuss some of the questions and concerns about how to achieve the benefits, while mitigating consumer risk.

We need to know if everybody who handles financial data is adequately protecting the privacy of their users. How do we ensure consumers aren't being misled about the acquisition and use of their data? And how do we empower consumers so they are in control of their data?

Today's discussion has never been more relevant, and I look forward to hearing our witnesses' testimony, and input from my colleagues.

With that, I recognize my friend, the new ranking member, Mr. Emmer, for 5 minutes for an opening statement.

Mr. EMMER. Thank you, Mr. Chairman. Thank you for your warm welcome. As you said, be careful what you wish for, right? You might just get it. I want to thank you for convening this hearing as well.

As the new FinTech Task Force ranking member, I look forward to working with you to bring more education and awareness to Congress about the new innovations in financial services. I very much appreciate this opportunity to help lead the task force in an effort to better educate Members of Congress on the emerging developments in technology that already have and certainly will continue to influence the entire financial services industry.

Today's hearing is about data, an individual's ability to control their data, and the practices that are utilized with this data. The Majority titled this hearing, "Banking on Your Data," and I expect we will have a lot of discussion today relating to privacy and security concerns, which are very important. But let's keep in mind that data can also benefit consumers and can empower individuals to own their own data and to leverage it when seeking services from companies.

The amount of data being generated is astounding. It is estimated that every day, we create 2.5 quintillion bytes of data, and that 90 percent of the data in the world today has been created in just the last 2 years. Not surprisingly, given Congress' inability to keep up with new technology, a TED Talk about how big data can produce insights on the work of Members of Congress and their interactions with each other was already featured more than 3 years ago.

As we have seen with the internet, information can be power. And when we are generating this amount of data, the owners and possessors of that data may gain that power. With that power may come increased responsibility and may impose an ethical duty use the data properly. Many companies have already realized these duties on their own and are benefiting from listening to their customers' demands. Standard-setting bodies like Financial Data Exchange are already bringing together fintech companies to create standards and limits to accessing data.

I appreciate, again, this opportunity for Members to learn about data practices and to increase the level of knowledge in Congress about the policies that companies use to innovate and to develop better services for their customers.

A broad unspecific definition of "big data" could also include the work that is already underway to digitize the services that the financial services industry already offers to all of us. This is the future, and there is no going back from here. We have seen this in several industries already, like music and other commerce. The future is in digital services. The question is, how do we empower the individual, as opposed to the government, to make the choices that are best for them?

I am hopeful this hearing will educate Members of Congress on the downside of big data but also about the benefits of data. Our job is to make sure that data helps empower the consumer and enables them to know what they are disclosing, when, and where. I hope this is a conversation more than a critique, and at the end

of the day, I hope this session is informative for members of this committee.

And I thank the chairman again for holding the hearing and looking at this issue objectively. I look forward to working together in a nonpartisan fashion to help Americans realize the benefits of this digital revolution and the help it can provide to each and every one of us. And I yield back.

Chairman LYNCH. The gentleman yields back, and I thank him for his remarks. And I do believe that this is an area where we can have great bipartisan cooperation and success.

Today, we welcome the testimony of our accomplished panel of witnesses. First, Ms. Lauren Saunders is associate director of the National Consumer Law Center (NCLC). NCLC is headquartered in Boston, in part of my district. And this year, it is celebrating 50 years of advocating for consumer justice and economic security.

Second, Dr. Seny Kamara is associate professor of computer science at Brown University, and chief scientist at Aroki Systems. His primary research focus has been cryptography and its applications to everyday problems in privacy and security. And at Aroki, he helps design encrypted data management systems.

Third, Dr. Christopher Gilliard is professor of English at Macomb Community College, and lab advisor at Digital Pedagogy. His work focuses on privacy and technology policy and the risk of discriminatory practices in algorithmic decision-making.

Fourth, Mr. Don Cardinal is managing director of the Financial Data Exchange, FDX, which is a nonprofit working group to set an industry standard for the secure transmission of sensitive financial data. FDX is an independent subsidiary of the Financial Services Information Sharing and Analysis Center.

And finally, Mr. Duane Pozza is a partner at Wiley Rein, where he advises on issues of privacy and data governance. Prior to joining Wiley Rein, Mr. Pozza was an Assistant Director in the Division of Financial Practice at the Federal Trade Commission's Bureau of Consumer Protection.

I want to thank you all for being here today.

Our witnesses are reminded that your oral testimony will be limited to 5 minutes. And without objection, your written statements will be made a part of the record.

Ms. Saunders, you are now recognized for 5 minutes for an oral presentation of your testimony.

**STATEMENT OF LAUREN SAUNDERS, ASSOCIATE DIRECTOR,
NATIONAL CONSUMER LAW CENTER (NCLC)**

Ms. SAUNDERS. Thank you.

Chairman Lynch, Ranking Member Emmer, members of the task force, thank you for inviting me to testify today on behalf of the low-income clients of the National Consumer Law Center.

I am going to focus my testimony today on the growing use of data aggregators to access consumers' bank account and other types of account transaction data, but my comments will also have applicability to other forms of data.

The use of consumers' transaction data has the potential to help consumers in a number of ways: to improve access to affordable forms of credit; to prevent fraud; to encourage savings; and to help

consumers better manage their finances. Companies are using transaction data to address problems that banks are not and to encourage banks to improve their own services.

I am especially intrigued by the use of cash flow data, which can help assess whether the consumer regularly has sufficient residual income at the end of the month to handle an additional expense. Cash flow data may especially help those with limited credit histories or those who have recovered from a temporary setback that is still reflected on their credit report. Cash flow data is currently only being used with consumers' explicit permission and generally to improve access or pricing, but I am concerned whether transaction data may become more routinely added to already robust credit reports, may be used to increase pricing, or may be monetized by the credit bureaus for other uses. These uses should be prohibited.

I appreciate that this data is being used today with consumer permission, but we should not put too much stake on consumer permissioning, which may be no more voluntary than clicking, "I agree," or saying yes to a potential employer who asks to review your credit report.

The intensely detailed personal and sensitive data inside consumers' accounts could also be used for less beneficial purposes. It may help predatory lenders refine their ability to make and collect unaffordable loans or it could enable targeting of consumers for harmful products. Transaction data can also be fed into algorithms and machine learning that may have results that lead to discriminatory impacts.

The use of data aggregators also poses concerns regarding security, privacy, and compliance with the Fair Credit Reporting Act (FCRA). A number of efforts are underway to address many of these issues, including the work of my fellow panelist, Mr. Cardinal from FDX, which we are in the process of joining. We support these voluntary efforts and dialogue, but ultimately, consumers cannot be confident that their data will be used appropriately unless the law clearly protects them across these different dimensions industry-wide.

First, security and protection. We need enhanced data security requirements and Federal supervision of entities that store significant amounts of consumer data.

Second, we need strong privacy laws that impose substantive limits on the use of information in ways that consumers would not expect, that ensure consumer choice and control are meaningful, and that do not preempt stronger State protections that may address new problems not yet addressed on the Federal level.

Third, we need to address misinterpretations of the Fair Credit Reporting Act by courts. New forms of information are essentially a consumer report that—if they are used for credit or other FCRA purposes, and consumers have a right to know what information is being used about them, to demand accuracy, to obtain corrections, and to be told if the information leads to adverse consequences.

Fourth, we must actively look for and prevent discriminatory impacts in the forms of new data. As recent news shows, computers can discriminate too.

To paraphrase the words of one fintech lending club, the disparate impact regime is an innovation-friendly approach that addresses concerns about discriminatory impact, while flexibly accommodating innovations without onerous compliance. Beyond fair lending, we need laws to prevent discriminatory impact in areas other than credit.

Finally, the Consumer Financial Protection Bureau (CFPB) can and should play a bigger role by supervising data aggregators for compliance with all laws within their jurisdiction, which should be expanded to include privacy and data security standards.

Thank you for inviting me to testify. I look forward to your questions.

[The prepared statement of Ms. Saunders can be found on page 62 of the appendix.]

Chairman LYNCH. Thank you very much.

Dr. Kamara, you are now recognized for 5 minutes.

**STATEMENT OF SENY KAMARA, ASSOCIATE PROFESSOR OF
COMPUTER SCIENCE, BROWN UNIVERSITY, AND CHIEF SCI-
ENTIST, AROKI SYSTEMS**

Mr. KAMARA. Chairman Lynch, Ranking Member Emmer, and distinguished members of the Task Force on Financial Technology, I appreciate the opportunity to testify at today's hearing on the role of big data in financial services. I will speak about how data is transforming the financial industry and how this transformation holds great promise but, unless it is carefully guided, also has the potential to erode consumer privacy and increase discrimination.

The financial industry is using new data sources called alternative data. For example, credit reporting agencies are using data about utility bills to create new credit scores. Insurance companies are using internet of things (IoT) data from homes and cars to better predict risks. Insurance companies have used Facebook posts and psychometric tests to assess people's risk profiles. Payday lending apps track location to determine how much time their users spend at work. Microlending apps are using location data, social media contact lists, and the behavior of Facebook friends to estimate people's creditworthiness. An app made in California that operates in Kenya even accesses call history under the belief that people who regularly call their mothers are more likely to repay their loans.

In addition to leveraging new sources of data, the financial industry is processing data in new ways using machine-learning models to make automated decisions quickly and at scale. While classical algorithms are designed by domain experts and expresses a series of rules and explicit choices, machine-learning models are produced by algorithms that learn from data. The models produced in this manner can be very effective in certain contexts but suffer from important limitations.

The first is a lack of transparency. We often do not know and, therefore, cannot explain why a machine-learning model makes a particular decision. This is a serious concern in the context of credit since the Equal Credit Opportunity Act (ECOA) and the Fair Credit Reporting Act (FCRA) require creditors to explain the reason an application was denied.

The second important limitation of machine-learning models is bias in decision-making. While this kind of algorithmic discrimination has been well-publicized, it is important to note that we are only in the very early stages of understanding the behavior of these algorithms. In fact, in that space, there are currently more questions than answers, so it is important to tread carefully.

Fintech apps can make use of multiple sources of consumer data, ranging from financial records provided by a bank to location data provided by a mobile device. Traditionally, financial apps have shared data through a practice called screen scraping. It is widely accepted that this practice is substandard from a privacy and security perspective, which has motivated the financial industry to develop Application Programming Interfaces (APIs).

Roughly speaking, an API is a standard interface between apps that allows for easier interoperability and improved security. APIs are a considerable improvement over screen scraping, but they are far from enough to guarantee consumer privacy. With an API-based design, apps can still access, lose, exploit, and abuse raw user data, and as long as consumers have to trust data-hungry apps that scour their sensitive data under vague privacy policies, they will never have real privacy.

But what if consumers did not have to give up their data in order to benefit from financial and technological innovations? What if financial apps and services never had to see raw data? This might sound impossible but, in fact, it is possible. Over the last 30 years, cryptography researchers in academia and in industry labs have developed a wide array of cryptographic techniques to process encrypted data. This gives us the ability to run algorithms, including machine-learning algorithms, over encrypted data, to search through encrypted files, and to query encrypted databases, all without ever decrypting the data.

The set of privacy technologies, which includes secure multiparty computation, private set intersection, homomorphic encryption, and encrypted search algorithms, can enable truly private data processing.

I want to stress here that this is not science fiction. These technologies are already in use today. By leveraging these advances in cryptography, financial technologies could deliver on their promise to improve the financial health of their customers without them having to sacrifice their privacy.

The financial industry is being transformed by technology, and in the wake of this transformation, it is easy to get carried away on a wave of technological optimism. As a computer scientist, I believe in the power of technology, but I am also acutely aware of its potential harms. As a cryptographer, I worry deeply about the erosion of privacy that these financial apps and services can cause.

We are all aware of the constant occurrence of data breaches, of the weaponization of private data to micro-target people and affect their behaviors. Do we want another Equifax? Do we want another Cambridge Analytica? Moving fast and breaking things is not sound engineering practice, and it is not sound policy. It is imperative that we proceed carefully and that we oversee this transformation with strong privacy laws and strong privacy technologies.

Thank you, and I look forward to answering your questions.

[The prepared statement of Dr. Kamara can be found on page 48 of the appendix.]

Chairman LYNCH. Thank you, Dr. Kamara.

Dr. Gilliard, you are now recognized for 5 minutes.

STATEMENT OF CHRISTOPHER GILLIARD, PROFESSOR OF ENGLISH, MACOMB COMMUNITY COLLEGE, AND DIGITAL PEDAGOGY LAB ADVISOR

Mr. GILLIARD. Chairman Lynch, Ranking Member Emmer, and members of the task force, thank you for inviting me to appear before you and provide testimony.

My name is Dr. Chris Gilliard, and I have spent the last 6 years studying, teaching, and writing about digital privacy and surveillance. I focus on the ways that digital technologies perpetuate and amplify historical systems of discrimination.

Too often, digital technologies render systems invisible and inscrutable under the guise of proprietary code, black box algorithms, or artificial intelligence. There are now countless documented examples of algorithmic discrimination, data breaches, violation of consumer privacy, and extractive practices on the part of platforms.

Moving forward, the onus for addressing these problems should be shifted onto companies so that, before they move their product to market, they provide evidence that they will not bring harm to the consumer, much in the same way food and drug safety operate now.

It may not be possible or useful to define the distinction between financial big data and all other data. Financial big data plays a role not only in finance, insurance, and real estate, but also in employment, transportation, education, retail, and medicine. In addition, third-party data brokers accumulate all manner of data to the point that even if there are categories of data that are protected, processing massive amounts of data often creates the existence of proxies that allow for discrimination against protected classes within or among systems that may not appear to be financial.

The primary reasons that many remain unbanked are because of historical inequality. While new forms of banking and credit may provide access to systems those people have traditionally not had access to, many of these technologies also offer these benefits in exchange for people's privacy or create opaque systems that offer consumers little opportunity for redress.

It is telling that the Apple Goldman Sachs card received so much interest, because opaque algorithms affect marginalized populations all the time. Yet, they do not have the reach and power to trigger massive media attention and an investigation by the State. For rich folks, algorithmic opacity may mean being denied a larger credit limit. For the poor, this may mean paying for medicine, shelter, or food.

The notion that companies like Facebook, Google, or Amazon are entering into banking in order to benefit the unbanked or people who do not have access to traditional credit markets is absurd on its face. As one recent report stated, for Google, the bank partnerships will give the tech behemoth a better ability to show advertisers how marketing dollars spent on its system can drive purchases.

There are two crucial frameworks for understanding these technologies and their impacts on marginalized communities: digital redlining; and predatory inclusion. Digital redlining is the creation and maintenance of technology practices that further entrench discriminatory practices against already marginalized groups. One example would be that Facebook ad targeting could be used to prevent Black people from seeing ads for housing.

“Predatory inclusion” is a term used to refer to a phenomenon whereby members of a marginalized group are offered access to a good, service, or opportunity from which they have historically been excluded, but under conditions that jeopardize the benefits of that access. The process of predatory inclusion is often presented as providing marginalized individuals with opportunities for social and economic progress; but in the long term, predatory inclusion reproduces inequality and insecurity for some, while allowing already dominant social actors to derive significant profits.

As an example, we might look at the report on the cash advance app Earnin, which offers loans for which users are able to tip the app. As reported in the New York Post, if the service was deemed to be a loan, the \$9 tip suggested by Earnin for a \$100, 1-week loan, would amount to a 469 percent APR.

As Princeton Professor Ruha Benjamin has argued, our starting assumption should be that automated systems will deepen inequality unless proven otherwise. Because of how algorithms are created and trained, historical biases make their way into systems even when computational tools don’t use identity markers as metrics for decision-making.

Further, the notions of consent, notice consent, or informed consent as they are currently constructed are not sufficient for a number of reasons. Privacy policies mainly serve to protect companies. Credit scoring companies operate without the express consent of the consumers they purportedly serve. Data is extracted, collected, combined, processed, and used in ways that go beyond the stated purpose to provide consumers. There is often limited accountability for when they have been irresponsible with consumer data. Companies rarely disclose and consumers even more rarely understand the full range and uses for their data.

We must reject the notion that regulations stifle innovation, as those harmed during innovation phases tend to be the most marginalized, and only later are policies addressed with no repairing of harms. The idea that corporate innovation, rather than the rights of historically marginalized groups, is an interest that Congress must protect turns ideas of citizenship and civil rights upside down. That these systems are proprietary often make the harms more difficult to detect.

Thank you.

[The prepared statement of Dr. Gilliard can be found on page 42 of the appendix.]

Chairman LYNCH. Thank you, Dr. Gilliard.

Mr. Cardinal, you are now recognized for 5 minutes.

**STATEMENT OF DON CARDINAL, MANAGING DIRECTOR,
FINANCIAL DATA EXCHANGE (FDX)**

Mr. CARDINAL. Chairman Lynch, Ranking Member Emmer, and members of the task force, thank you for the opportunity to offer testimony at this hearing. My name is Don Cardinal. I am the managing director of Financial Data Exchange (FDX).

FDX was formed just a little over a year ago as an industry-led collaboration that includes financial institutions, financial data aggregators, fintechs, industry organizations, consumer advocacy groups, and permission users of financial data. The mission of FDX is to unify the financial services industry around a common and interoperable royalty-free standard for the secure sharing and convenient sharing of financial data with financial technology applications, fintech apps. We are guided by five core principles: control; access; transparency; traceability; and, of course, security.

Over the last decade, technological innovations in financial services have empowered consumers to better understand where and how they spend their money, increase their credit scores, prepare their taxes, verify accounts and balances, and aggregate disparate financial accounts. While consumers have benefited immensely from these innovations, they primarily come through a mechanism known as screen scraping, and only done through the sharing of consumers' IDs and passwords at their financial institution.

Screen scraping is the automated process of collecting the text that appears on a website for the purposes of another application. For example, online banking websites display customers' account balances and transactions, and this data can be retrieved through a permission fintech app or a data aggregator by an automated login on the customers' behalf and present that data in some other application. And while screen scraping has provided a useful avenue for consumers to use and share their own financial data, it is very inefficient and can lead to poor data quality. This technology also places undue stress on financial institutions' tech stack through the sheer volume of automated logins.

And, finally, the needed sharing of sensitive login credentials and the lack of consumer control over the amount of data they share with other parties means it is really time to move on from screen scraping.

In recognition of these challenges, FDX was formed to promote a better way forward, namely, moving the financial services industry away from screen scraping and to the adoption of the use of APIs for access for consumers' financial data. Now, API simply means "application programming interface", and in layman's terms, it is just a way for computers to talk to each other with a common format. They also make consumer-permission data sharing easier, more accurate, and more secure, because they lay out in detail the rules for how to request data and exactly what data will be returned.

Our chosen standard is aptly named the FDX API. It allows for users within the financial data ecosystem to be security-authenticated but without sharing or storing of the login credentials with third parties. So instead of a fintech or aggregator logging in on behalf of a customer with their shared credentials, an API allows the consumer to log in themselves, and be authenticated by their own

financial institution. It gives the consumer the ability to permission their data for the chosen app. In fact, through the broad adoption of the FDX API, screen scraping will eventually cease, but the flow of user permission data will encounter less friction and be even more secure and reliable than ever.

So with that overview out of the way, I want to use my remaining time to highlight a few key points for the task force this morning, and I have attempted to expand upon these in my written testimony.

First, the only consumer financial data that will be accessed with the FDX API is that which the consumer has expressly consented to, and permission to share with fintech apps. This eliminates access for so-called data brokers who collect vast amounts of data, often without consumers' knowledge or consent.

Second, FDX is working towards specific-use cases for fintech apps to minimize the amount of data that consumers require to share for a given use. While screen scraping currently allows really any data on a consumer's website to be collected, defined-use cases through the FDX API limits the collection of data to only that which is needed to fulfill a specific purpose; and by minimizing data in play, you maximize privacy.

And, third, FDX represents the entire consumer financial services ecosystem, which includes small fintechs, local banks, credit unions, all the way up to the largest financial institutions, and consumer advocacy groups. Further, the FDX API provides a framework necessary to provide scaleable technology solutions so that even the smallest financial institutions will be offered the same goods and services as the largest financial institutions, but at a fraction of the cost. The FDX API is, after all, royalty-free in perpetuity for all parties.

In sum, FDX represents the financial services ecosystem coming together to put the consumer in the driver's seat regarding the use and sharing of their own data. Demand has been a leading force for this massive innovation that has taken place, and we believe the entire financial system ecosystem is best positioned to ensure that these consumers are empowered but have the tools to share and use their own data in the most secure manner possible.

Thank you for the opportunity to speak this morning.

[The prepared statement of Mr. Cardinal can be found on page 32 of the appendix.]

Chairman LYNCH. Thank you, Mr. Cardinal.

Mr. Pozza, you are now recognized for 5 minutes.

STATEMENT OF DUANE POZZA, PARTNER, WILEY REIN

Mr. POZZA. Chairman Lynch, Ranking Member Emmer, and members of the task force, thank you for the opportunity to appear today to discuss the role of big data in financial services.

I am a partner at Wiley Rein, where my practice includes advising companies on the legal and regulatory framework for collecting, using, and managing consumer data, including in financial services and counseling on U.S. and global privacy laws. This includes emerging regulatory approaches around machine-learning technologies which depend on large and sophisticated data sets. I pre-

viously worked at the Federal Trade Commission on financial technology issues.

Data-driven financial services hold enormous potential to improve consumers' financial lives. Companies can use consumer data responsibly to expand access to credit, provide customized financial advice, detect and prevent fraudulent behavior, and provide financial services at a lower cost, among other advantages. Companies are already using large and robust data sets to accomplish these objectives, and the development of machine learning and AI technologies will further advance what these technology innovators can accomplish.

Companies using consumer data in innovative ways for financial decisions operate in an area that already has many significant laws and regulations on the books and multiple regulatory authorities. Companies must comply with well-established financial services laws, many of which implicate the use of consumer data, in addition to Federal Trade Commission (FTC) guidance on data privacy and security. Applicable Federal laws include the Fair Credit Reporting Act, the Equal Credit Opportunity Act, the Gramm-Leach-Bliley Act, and the FTC Act Section 5 authority and prohibitions against deceptive or unfair practices, all of which also apply in the context of big data.

The companies must also comply, to varying degrees, with consumer privacy laws that reach across sectors, both on the international level—for example, the European Union's General Data Protection Regulation—and on the State level—for example, the California Consumer Privacy Act. State laws, in particular, threaten to create a piecemeal compliance framework and burden businesses that already have substantial compliance obligations, including in the area of big data.

The experience with California's law illustrates some of the challenges that companies face. As consumer data is increasingly used to provide better financial services, it is important to carefully consider consumer expectations and preferences around use of their information and weigh the benefits that better financial services can bring and the cost of added regulation.

The use of advanced data for credit decision-making is particularly promising. Large data sets can enable lenders to better analyze credit risk and potentially expand access to credit to those who find it difficult to obtain credit when evaluating using traditional credit models. Many consumers are thin-file or no-file consumers who lack an adequate credit history to generate a reliable credit score, and others have relatively low scores that do not accurately reflect their level of creditworthiness.

The nonprofit, FinRegLab, recently released the results of a promising study that illustrates the ability of large-scale data analytics to responsibly expand access to credit without raising issues related to bias. FinRegLab analyzed data from six non-bank financial services providers that used cash flow information as part of their credit decision-making. The organization study concluded that participants appeared to be serving substantial numbers of borrowers who may have historically faced constraints on their ability to access credit and, in regard to fair lending, that the degree to which the cash flow data predicted credit risk appeared to be rel-

actively consistent across subpopulations of race, ethnicity, and gender, and appeared to provide independent predictive value across all groups rather than acting as proxies for a demographic group.

Top officials at the Consumer Financial Protection Bureau (CFPB) also recently announced the results of the Bureau's data analysis conducted in connection with its no-action letter to Upstart Network. Upstart's underwriting model uses a range of data and machine learning in making credit underwriting and pricing decisions. The agency found that the company's tested model approved 27 percent more applicants than the traditional model, and yielded 16 percent lower average APRs for approved loans. It also showed no disparities that the CFPB found to require further fair lending analysis under the company's compliance plan.

These are just some examples of how financial services companies are using consumer data responsibly to provide better financial services for the benefit of consumers.

Thank you. I look forward to your questions.

[The prepared statement of Mr. Pozza can be found on page 54 of the appendix.]

Chairman LYNCH. Thank you very much.

I now yield myself 5 minutes for questions.

One of the most helpful books in this area is a book called, "The Age of Surveillance Capitalism," by Professor Shoshana Zuboff. I think she is at Harvard. She talks about how all of these platforms are soaking up what she calls behavioral surplus, everything we do, what we read, who our friends are, how we drive. Our cars are now hooked up. Some insurance companies are actually monitoring our driving so they know when you are driving like a nut to get your kids to school in the morning, and they jack up your rates subsequent to that.

One of the things that she pointed out was the pernicious terms of agreement that a lot of these apps have, that they might be framed as privacy agreements, but they are actually a lack of privacy agreement. In other words, you give away your privacy. In order to get on that site and get access, you click, "I agree," to very long, very complicated terms of agreement, an access contract. And I have a few of them here.

Mint, which is a somewhat popular financial management tool, I scrolled down that to see what I had agreed to, to get on that site—37 pages long, 11,312 words. Ridiculous.

Venmo, which is really popular, I use that on occasion. I just clicked, "I agree," because I couldn't—13,196 words, 40 pages, and really dense legalese. I am an attorney, and it was tough to get through.

Qapital, with a "Q," that is a savings application—almost 10,000 words, 10 pages, but really, really dense.

Dr. Kamara—actually, for any of you, I think you all get a sense of this. How do we instill in consumers the knowledge of what they are agreeing to in terms of clicking, "I agree?" I have two young girls. One is in college, and one is just graduating college. And that iPhone in their life is just absolutely necessary. So, they are going to click, "I agree." I just know they are. Like millions of other American kids and kids all around the world, they are just going

to—in order to get on that site, you have to click, “I agree,” and you have to let them take your data and resell it.

How do we convince consumers of the seriousness of what they are doing? And what rules might we put in place to balance the scales here so that you don’t have to sign away your firstborn in order to get access to some of these sites? How do we challenge that?

Ms. Saunders?

Ms. SAUNDERS. I think ultimately, these are not issues that can be disclosed. At the end of the day, I don’t really think it is possible for consumers to fully understand how their data is going to be used or, frankly, have the option. I may understand what happens when an employer checks my credit report, but if I want the job, I am going to have to say, yes, you can check it.

As use of data becomes more widespread, we are not going to have the choice. I, too, have spent some time looking at privacy policies, and I thought I was a relatively sophisticated consumer, but I can’t understand them. And even if you simplify them, even if you use the model form, at the end of the day, what does it mean, well, we only use your data to the extent necessary to provide our service? I don’t know what that means.

I think at the end of the day, people need to have confidence that the data is going to be used in ways that people would expect, that would be logical for the service at hand, that a minimum amount of data is being used. And that is some of the efforts that FDX is undertaking to try to figure out use cases. They don’t have—

Chairman LYNCH. All right. Thank you. I only have 45 seconds left.

Dr. Kamara, so does that mean we have to basically surrender all our data in order to just—we lose control of all of our data and that is just a fact of life?

Mr. KAMARA. No, it doesn’t—it is not required. We have technology. We have ways of designing apps and services so that consumers don’t have to give up their data, so that services can be provided without having to see raw data. This is technology that has existed for about a decade that is practical today, but because companies never really had an incentive to improve their privacy practices, it has been underinvested in, but it is not necessary.

Chairman LYNCH. Thank you.

Dr. Gilliard?

Mr. GILLIARD. The onus should not be on the consumer to ensure that they are not being exploited.

Chairman LYNCH. Okay. My time has expired.

I am going to yield to the ranking member, Mr. Emmer, for 5 minutes.

Mr. EMMER. Thank you, Mr. Chairman. And thanks again to this great panel.

Mr. Cardinal, does the average consumer utilizing fintech services know to what extent their financial and personal data is being stored and shared?

Mr. CARDINAL. Let me take that in a couple of different ways. Our key principles are control, access, and transparency, and I want to talk about transparency. The idea that a consumer should know what data elements they are sharing, for what purpose, and

for what duration, is key to what we are doing. And as NCLC pointed out, I think that is a driving principle.

Customers should be able to make an informed decision about what data they are sharing, whether they are trying to get a discount at the grocery store or for other purposes. At the end of the day, it is their data. The customer should remain in control, and an informed consumer, I think, makes the whole industry better.

Thank you.

Mr. EMMER. Yes, but they don't know. At the end of the day, they don't know how much of it is being taken and how much of it is being shared.

Mr. CARDINAL. I believe if you disclose exactly the purpose—I want to file my taxes and I am going to download my tax forms, I think that is fairly clear. To the extent we can disclose it, we can do that initial piece. Now, where it goes from there after, we really can't be responsible, I think, as Ms. Saunders pointed out.

Mr. EMMER. So when consumers—Mr. Cardinal, let's just continue on this. When consumers authorize screen scraping by giving away their user name and password, what risks are they exposing themselves to?

Mr. CARDINAL. Again, we are moving away from screen scraping. The whole idea is to get away from that, get away from what we call held-away IDs and passwords, because if you don't share it, you can't lose it, the whole idea of reducing the whole risk envelope.

So screen scraping, again, also is access, as I mentioned in my testimony. You have access to the entire scope of data, it is visible to the naked eye, whereas the use cases that we are developing minimize data, and the NIST standards that the government follows stress data minimization as a way to reduce risk. So we are trying to go to an API with defined-use cases with minimized data and without held-away credentials to really reduce that entire risk surface for everybody.

Mr. EMMER. Thank you.

Ms. Saunders, how does the Gramm-Leach-Bliley Act define financial institutions? Do fintech companies, data aggregators, and data brokers clearly fit the definition?

Ms. SAUNDERS. I am not an expert on the Gramm-Leach-Bliley Act. I do know that it covers traditional financial institutions such as banks and credit unions and also some other entities that are not banks and credit unions, but it is not nearly broad enough to cover the wide range of companies that do have our data and implicate data security and privacy concerns.

Mr. EMMER. Should a consumer be able to make portable all of the data available to them via their native online banking account or is that on their paper statement to a third-party service provider, or do you believe that only a subset of that data may be leveraged by a consumer?

Ms. SAUNDERS. I think it really depends on the use case. I think one potential future use of accessing account data would be to make it easier to port over your data to a new account, comparison shop and to—it is very difficult to unenroll in all of your online bill pay. On the other hand, there are uses today where people should be able to use it for cash flow underwriting and other things.

Mr. EMMER. Okay. For the panel, I am a huge supporter, as I believe probably everybody up here is, of individual privacy, and I have some concerns about some firms' data hygiene practices. What do you see in the next 5 to 10 years in terms of how big data is going to transform financial services? Any of you may answer.

Or was that too broad? Was that the ocean? And if that is too difficult, let's narrow it. Do smaller banks have the resources to comply with the new regulatory regime under data privacy laws like the Gramm-Leach-Bliley Act? And maybe this is for Mr. Pozza?

Mr. POZZA. I would say that what experience with the California Consumer Privacy Act is showing is that smaller companies in general are having difficulties with compliance. I think that the law itself has some ambiguities and is not written in a very straightforward manner, and illustrates the problem of regulating around this space in a broad brush, and the smaller companies are incurring compliance costs.

Mr. CARDINAL. Ranking Member Emmer, I would like to add on, since the FDX API is royalty-free, it levels the playing field. A mom-and-pop credit union can offer the same access to data as a top-four universal bank. And a lot of these credit unions rely on core processors, and one of them is on our board. We are working with the other ones. So once the cores get onboard and offer this API, a lot of the credit unions in your district, and in my district, will be able to offer this same type of royalty-free access that is secure and is much more reliable than screen scraping.

Mr. EMMER. Thank you. I see my time has expired.

Chairman LYNCH. The gentleman yields back.

The gentleman from Utah, Mr. McAdams, is now recognized for 5 minutes.

Mr. MCADAMS. Thank you, Mr. Chairman, for holding this hearing. And thank you to the witnesses for your testimony today.

I am fascinated by this topic and the myriad of connecting issues related to it—big data, data security, privacy, data ownership—and how all of this interacts with innovations in financial services, as well as potential risks to consumers, because I do see great potential benefits but I also recognize the potential risks in terms of data security, and discrimination in lending, for instance, among other issues.

So first question, Mr. Cardinal, I know in the various testimonies or even in many of the conversations that occur in Congress, definitions matter, and being specific with what companies we are referring to, that also matters. Can you explain or maybe even highlight the difference between a data aggregator and the role that they play in the financial services industry and the role a data broker plays?

Mr. CARDINAL. Thank you for that question, and I appreciate the chance to straighten out or expand upon some ambiguity in the press.

A "data aggregator" is simply a data service company that allows any third party that is permissioned to reach out and extract, with consumers' consent, data from a variety of sources, whether it be a bank, a brokerage, or an investment company. A "data broker" is someone who is gathering data, harvesting quite a bit of data, often without the customers' knowledge or even consent. So, there

is a clear difference, and that has to do with customer awareness and permission.

Mr. MCADAMS. How do the regulatory or legal obligations of those two entities differ?

Mr. CARDINAL. I will leave the technology standards bias. I really couldn't comment on that part. I'm sorry.

Mr. MCADAMS. Do any of the other witnesses have any thoughts on that?

Okay. I just want to maybe ask a further question. Does whether the data is consumer-permissioned or even revocable access change how we should view the data and the entities holding or transmitting the data? Because that seems to be fundamental in the distinction between those two, the data aggregator and the data broker.

Mr. CARDINAL. You are spot on. Consumers should be in control. We are all here to serve the consumers, and the idea that they should have clear knowledge of what data they are sharing, for what purpose, and for what duration—and I will give you an example. I am a CPA by trade, and the idea that, yes, I want to share my tax forms with TurboTax through April 15th is very clear and very conspicuous versus data that I don't even know is being used.

Mr. MCADAMS. I guess that leads to my next question, and it would be for anybody on the panel.

I have an iPhone and have numerous apps and websites that I use, some infrequently, and some on a regular basis. And I am positive that I have given access to various bank accounts or financial data, other personal data, to dozens of different companies. That is probably a conservative estimate. But as a consumer, I honestly don't know and probably can't even easily locate who has access to my data and how it is being used right now. I don't even know how long ago I may have given access or how long that access may be for.

So how should we as policymakers think about this issue? And are there ways, either through the government or through private sector standards that could better promote consumer awareness and/or consumer control over this information?

Ms. SAUNDERS. I can address that.

Mr. MCADAMS. Thank you.

Ms. SAUNDERS. Ultimately, I think that we need to have rules that data is used in ways that consumers expect, so that you don't have to decipher how it is going to be used. I think permission should also expire after 1 year.

I was surprised when I got an email alerting me to some access for something I signed up for years ago. So often, if you apply for credit, you think that is going to be used at the moment of the credit application, and you don't realize it may be used on an ongoing basis. There may be uses that you just have no idea about.

So, minimizing the amount of data, requiring it to be used in ways that are logical for the use, and putting an end point so consumers can have control and decide whether to reauthorize the use or not.

Mr. MCADAMS. And is that a place that we should look at as policymakers, as Members of Congress, to ensure that those standards are equal and fair and apply across the industry?

Ms. SAUNDERS. Yes, I think so. There are voluntary efforts to address principles like that, which is great in the current situation, but ultimately, we want this applying across all uses and not just those who choose to comply.

Mr. MCADAMS. Mr. Kamara?

Mr. KAMARA. I would just like to add, the principles that Ms. Saunders describes can be embedded in the technology. They can be embedded cryptographically so that data is always protected mathematically. So it is possible to design these services and these apps so that your data will never be seen by any of the data aggregators or financial services that need it in order to build their products.

Mr. MCADAMS. Dr. Gilliard?

Mr. GILLIARD. As Chairman Lynch noted, this is sort of the age of surveillance capitalism, so most companies generally operate from a collect-it-all, keep-it-as-long-as-possible perspective. And, again, I think that there do need to be more regulations, because it is an unfair burden on consumers to take weeks or months to read the dense kind of language that is in these policies.

Mr. MCADAMS. Thank you. I see my time has expired. I yield back.

Chairman LYNCH. The gentleman yields back.

The Chair now recognizes the gentleman from Missouri, Mr. Luetkemeyer, for 5 minutes.

Mr. LUETKEMEYER. Thank you, Mr. Chairman. And I thank the panel today. It is quite interesting.

Mr. Pozza, your testimony states that the California attorney general is currently accepting comments on rules to enforce the California Consumer Privacy Act (CCPA), and those rules are scheduled to go into place in July of 2020. However, the CCPA's date of enactment is January of 2020, so they are getting the rules after the enactment. I am not sure how that works, but hopefully you can explain it to me here in a second.

In addition, you highlight how financial institutions are unclear what personal information they possess is covered by this vague law. Lastly, I heard from financial institutions that some provisions of CCPA are in direct conflict with other State laws regarding data security and privacy.

All that being said, I have a simple question: How are financial institutions supposed to comply with CCPA?

Mr. POZZA. I think it has been difficult for financial institutions to navigate CCPA compliance. As I point out in my testimony, and as you state, the law has an effective date of January 1st, but the regulations are still being finalized. We are in the middle of a comment period for the draft attorney general regulations, which would go into effect, at the latest, on July 1st. This means there is a current set of rules that are themselves a bit unclear. They are in the law, and then those can change or become more detailed or even be expanded, depending on what the attorney general does in the regulations.

That makes it very difficult for financial institutions and other companies to figure out how to essentially manage their data practices, because this is really a broader issue of sort of data governance. It is what obligations are you going to have to consumers

about their certain data to respond to certain requests and how you deal with it with third parties.

So, these are difficult issues to go through and think ahead to how the law could be changing over the next—obligations could change over the next 6 months.

Mr. LUETKEMEYER. Thank you for that.

I know that all of this data—the world of technology is wonderful. It allows us to do so many wonderful things and speed things up and give people more access to their own information, but it is also scary from the standpoint of what can happen to it. The data aggregators are really something that I am very concerned about.

As somebody who comes from the other generation—I still have a rotary phone, by the way. So for those of you, any millennials in the audience, and maybe some of you on the panel, if you can figure out how to do a text message on that, I would sure appreciate it. I'll be glad to see you after this hearing.

But I was discussing it the other day with an entity who lost hundreds of millions of dollars because of the data aggregator doing some nefarious things. They had access to individuals' information because they had given it to somebody along the way, whether—Mr. Cardinal, you talked about tax preparers a while ago—and suddenly, they use a third party to be able to access all that. And now, they can go in and they can scrape the screen and get—and nightly, what this entity was telling me, was that 80 percent of the transactions that go on in there overnight are from data aggregators. They have had to up the amount of computer power in their business to be able to accommodate the data aggregators that are coming in every night and scraping all the information off. It is not their own customers; it is the data aggregators.

This has gone way beyond access to information. And so, while I am not a big fan of regulation, there is a whole system out there right now that looks to me to be out of control, and we are going to have to figure out how to put the genie back in the bottle so we can protect our consumers and allow them to access their information.

I know you have talked at length here about this, but do you want to elaborate a little bit more on that, Mr. Cardinal?

Mr. CARDINAL. Yes. Thank you for the opportunity to address that. That was part of the reason FDX has stood up. And we have banks, brokerages, investment firms, data aggregators, and fintechs, the whole ecosystem working together on this issue. Nobody likes screen scraping. It is inefficient. It is expensive. It can lead to inaccuracy in data occasionally.

The API is much more secure, and my colleagues here have mentioned that several times. You limit and control the amount of data. It is an order of magnitude and more efficient.

The hardware costs alone that you referred to come down by an order of 100X, and it makes the front-door defense also a lot easier by ceasing screen scraping. That means anything hitting your front door should only be human. So, that helps your cyber posture. It helps your data risk posture. It helps your hardware cost posture. And again, it limits the data out there in play and, of course, it removes IDs and passwords held away. This is the end state that ev-

everyone is working toward, whether you are a bank or a brokerage or you are an aggregator or a fintech.

Mr. LUETKEMEYER. The chairman asked a while ago the question about, how do we get consumers to understand the seriousness of this. We have had former Director Cordray of the CFPB in this very room, and he indicated that the CFPB was collecting 80 percent of all the credit card transactions in the country. They are collecting that data. That should scare the bejeebers out of every single person here today.

My time is up, but I want to thank the panel for being here today. You have been very informative, and I sure appreciate your efforts. Thank you very much.

And I yield back.

Chairman LYNCH. Great questions. Thank you.

The gentleman from Florida, Mr. Lawson, is now recognized for 5 minutes.

Mr. LAWSON. Thank you, Mr. Chairman. And I welcome the witnesses today.

Are there any examples in the market today to which consumers and our small businesses might not be permitted to access the financial data which might impact their products or services? This is for anyone who cares to respond.

So, there is none?

Tell me this, how does big data collection impact consumer profiling?

Ms. SAUNDERS. I would say we don't know, and that is the problem. We have all sorts of data that is fed into big black boxes and algorithms, and we don't know how it is being churned and correlated and conclusions are being drawn, and we really don't understand how it is being used.

Mr. LAWSON. Okay. A little bit of a follow-up, with the increase of big data comes an issue of security. Can you share how consumers will know who has access to their data and how the information will be shared?

Ms. SAUNDERS. Again, I don't think it is something that consumers are equipped to know, and we shouldn't put that onus on the consumer. We should have rules about what can be shared and rules about how data is held securely and not put it on consumers to figure out who is holding their data securely or not.

Mr. LAWSON. Mr. Cardinal?

Mr. CARDINAL. We are seeing some innovation in the industry around making the data sharing more transparent. If you look at Wells Fargo's control tower, you can see—and I will pick on TurboTax again, because I am an accountant and I like to do that. You can see, yes, I have permission from TurboTax to pull my data down, and you see other firms standing up dashboards where consumers can see very clearly whom they permissioned, and it gives them the ability to kill that connectivity at any time. So, you have firms like USAA or Bank of America or Citibank, and they are also standing up those dashboards because they want to inform consumers well and give the consumer the ability to kill that connectivity at any time.

Mr. LAWSON. Mr. Gilliard?

Mr. GILLIARD. As Ms. Saunders has said, there is very little ability—I know a lot of computer scientists, cryptographers, people in privacy and surveillance, and even people with advanced skills, and it is very difficult for them to know the answer to that question. But the other thing that is important—and Dr. Kamara alluded to this—it is very hard, and it is, in fact, impossible for people to know how that data is combined, processed, repurposed, and what kinds of correlations or connections will be made by companies who do this.

As Dr. Kamara said, so there is some correlation between calling your mom and paying your bills. So, only the people inside that system, and sometimes not even them, would know that correlation exists. People outside of it have absolutely no ability to know that.

Mr. LAWSON. Okay. Mr. Kamara?

Mr. KAMARA. I would also add that a lot of this data that is collected is used in ways which we really don't understand, and that the designers may not understand, because the machine-running algorithms can be inscrutable. But also, this data oftentimes is kept even after the service has been rendered. And the data is kept longer and it is kept to improve the systems of the companies that are providing these services, but we don't necessarily know how long this data is kept and for what purpose.

Mr. LAWSON. Okay. And whether this is appropriate or not, but recently in this committee, we talked about debt collectors. So, when there is outstanding debt and the data then is transferred over to the debt collector, how long are they able to keep the consumer information? Do you know that, Ms. Saunders?

Ms. SAUNDERS. I am not aware of any limits. And that was one of our concerns about the debt collection proposal. If debt collectors are texting people through WhatsApp, and Facebook actually sees those messages, are they going to use that data? Are they going to target people for debt settlement scams and other problems? We don't know what information gets collected and how it gets turned around and used.

Mr. LAWSON. When consumers sign affidavits, let's say getting a loan or have a substantial debt—and my time is about to run out—is there always something that they sign at the bottom which allows them to transfer all of the information to other collectors?

Ms. SAUNDERS. I think that information may be in the fine print. But consumers don't really know what is going to happen.

Mr. LAWSON. So it is as if the fine print is so small until people just really want to get credit or anything they want, forget about reading it until later on.

Ms. SAUNDERS. When consumers take on a loan, they don't expect to be hit by a debt collector. They take out a loan expecting they are going to repay it. And what happens later on is something that people aren't focused on at the moment.

Mr. LAWSON. Okay. I yield back, Mr. Chairman.

Mr. LYNCH. I thank the gentleman.

The Chair now recognizes the gentleman from Arkansas, Mr. Hill. Welcome back. And you are recognized for 5 minutes.

Mr. HILL. Thank you, Mr. Chairman. I appreciate you holding this hearing.

This is such a fundamental hearing, I think, for all of us in fintech, because big data is the fundamental building block for financial services now, and the providing of health services now. So, getting this right is very important.

And I have said since the beginning of our work in this Congress, that we can't really have a digital future in health or financial services or any other endeavor unless we get the data piece right so that we as individuals own our data, it is our data and we—as our panelists talked about, and we permission that data use individually for a health provider or financial services provider to provide us services, and that we also have an authentication system that values cyber protections and privacy and is not tied to a user name and my pet's name and my birthday year.

And all about that, we have heard this year that that is fundamental. So we control our data. It is our personal data. We use that data with our financial services providers. In turn, it is authenticated in a way that protects privacy and cyber risk. And those are just critical.

This gets to my friend from Missouri's line of questioning about—I want to talk as well about California and what we see. But we have one company in Arkansas that is called Acxiom, and for 50 years, they have sort of been a data bank for financial services companies. They have worked hard to do that in an ethical, secure, and legal way to protect consumers along the way. They have innovated there. They have used a lot of that data with financial services. They are now working on the California privacy law and how it can be implemented for their clients.

And so a question I have about California, probably following up on Mr. Luetkemeyer, Mr. Pozza, what do you think are the biggest shortcomings in that statute?

Mr. POZZA. I think one of the biggest issues around it is the sort of lack of clarity around the specific obligations, as I talked about before. A second piece of it is the way it treats financial institutions. It carves out data that is subject to Gramm-Leach-Bliley (GLB), but it does not carve out financial institutions, which means that it is layering another level of unclear regulation on top of data that is treated a certain way under GLB.

So what that means for a financial institution is they have to parse through, is this particular piece of data covered under GLB; and, if not, is it then covered under CCPA if it is related to California? That, I think, is confusing both to consumers and to companies to have data treated different ways under this piecemeal approach.

I think, in thinking about California, it is also instructive to look at the chance of other State legislation happening over the next year, and certainly there will be lots of bills introduced. So there is also a level of uncertainty there looking not just at what is California going to look like in a year, but what is any other State going to look like and is it going to build on top?

Mr. HILL. I support a national standard for privacy, and we have tried that here. I know Mr. Scott and I talk about this on a regular basis. We have to create a consensus to do that, and I think it is an important policy, as I say, not just in financial services, but across the government.

Mr. Cardinal, you suggest that APIs are critical to protecting this authentication piece and improving privacy. So in your work, are 100 percent of the consumers in your portfolio all covered by APIs?

Mr. CARDINAL. We are getting there. We are at—

Mr. HILL. What percent are covered by APIs?

Mr. CARDINAL. I would say, at this early stage, we just have raw numbers. I am not sure what the actual overall percentage is. I would say probably under a quarter. We surveyed our members and they indicated that 5¼ million had made the switch from old screen scraping tech to the new APIs, and they have estimated we will be at 12 million by April of next year. It is hard to know what the entire population is.

Mr. HILL. Do you think the bank regulators, the financial services regulators in the investments and banking should require all financial services data be covered by an API and not permit any form of screen scraping?

Mr. CARDINAL. We are a tech standards body. We are not going to comment on policy regulation, although we do inform the regulators on our progress and what we are doing on a voluntary basis. We were here just a few weeks ago, talking to the OCC, the CFPB, and Treasury, and they—

Mr. HILL. But it is a best practice, right? An API is a best practice?

Mr. CARDINAL. The Treasury said last year that APIs represented a big risk reduction over screen scraping, and we agree with them.

Mr. HILL. Thank you, Mr. Chairman. I yield back.

Chairman LYNCH. The gentleman yields back.

The Chair now recognizes one of our most active and thoughtful members on this task force, the gentleman from Georgia, Mr. Scott, for 5 minutes.

Mr. SCOTT. Thank you. Thank you very much, Chairman Lynch, and I appreciate those kinds words that you had to say, and I appreciate your leadership on this.

Mr. Hill is right, big data and privacy are critical to fintechs. Our technology now is moving at warp speed. Every day, it seems like there is something else we have to adjust, and I will tell you why: It has been 20 years since the enactment of Gramm-Leach-Bliley, which is the law predominantly governing the treatment of big data and privacy protection in all of the financials here. But since that time, we have seen extraordinary technological development that has changed the way consumers interact with financial services. And just in recent days, members of the Senate's Committees on Commerce, Science and Transportation, and Judiciary have released a set of privacy and data protection principles to underpin a broad privacy framework. And I am sure you all are probably aware of what the Senate has done. But among these principles are the minimization of the data collected, limitations on the way data can be shared between service providers and third parties.

So thinking about the way that our financial technology has evolved, and understanding how the value of data itself has increased, how can our great financial technology grow in a way that incorporates key privacy protections?

Mr. Cardinal, let me start with you.

Mr. CARDINAL. Thank you for the question. And I go back to our five core principles of control, where you put the customer in control of their data; transparency, so they know and see what is going on; and in a real way, traceability, access, and, of course, security.

Earlier, I talked about the National Institute of Standards and Technology (NIST). NIST sets a lot of the government framework for data control and cybersecurity, and one of their core principles is data minimization. And good risk governance mandates data minimization, and we have that in our security principles as well. And the use cases we are defining set out that you should only return the data necessary to achieve a particular purpose, for example, again, a tax return or doing budgeting. Only get the data you need to do that one thing.

So those five key principles really guide what we do, and I think they fit hand-in-glove with the points you raise.

Mr. SCOTT. Okay.

Mr. Kamara, in recent years, we have seen two major pieces of privacy legislation pass in California and in the European Union. These two pieces of legislation appear to shift towards what we call a bill of rights model in which a consumer can have a certain expectation of what privacy protections exist. Do you agree with this assessment?

Mr. KAMARA. Yes, I do. I also think that the excitement around financial technologies is great, but what I would like to see is as much excitement around privacy technologies. APIs are definitely an improvement over screen scraping, but I think we can still do better. We can bring minimization. We can minimize the amount of data collected down to zero if we invest in the right technologies.

Mr. SCOTT. In your opinion, in these two areas where this legislation impacted, how would you assess their progress?

Mr. KAMARA. I am a computer scientist. I am a cryptographer. So, this is not exactly what I work on every day. I think, from my vantage point, one of the benefits is that it is forcing industry to actually have to put in real, practical technological measures to protect consumers' privacy, and I think that is a very positive outcome.

Mr. SCOTT. And do any of you feel, in addition to you, Mr. Kamara, that any challenges have arisen with the implementation of these laws that may be helpful to us and instructive on a national basis?

Mr. KAMARA. I think there are surely challenges to implementing any policy, but I think these challenges are surmountable. We can use technology to do incredible things. We can use technology to provide privacy as well, so—

Mr. SCOTT. Do you feel comfortable that we are—

Chairman LYNCH. The gentleman's time has expired.

Mr. SCOTT. Thank you.

Chairman LYNCH. I thank the gentleman.

The Chair now recognizes the gentleman from Ohio, Mr. Davidson, for 5 minutes.

Mr. DAVIDSON. Thank you, Mr. Chairman.

This is an exciting time, because not all the time in this room do you have a near-uniform sense of what ought to be done. I haven't heard anyone say that the status quo with respect to pri-

vacy is just great. Everyone has said that it is broken, and everyone has said that there is a need to fix it.

I just listened to Mr. Scott and Mr. Hill speak about their common ground that they shared in terms of a Federal approach. We haven't yet seen that bill and, unfortunately, this committee doesn't have full jurisdiction over everything. But what does have full jurisdiction over privacy? We don't need a new bill of rights with respect to privacy. I don't think there is an expiration date on the Fourth Amendment. Let me read it for you:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

This was originally a restriction on the Federal Government doing these things but, of course, as we know, the Fourteenth Amendment ruled that out through all of the States. And I believe that Louis Brandeis in *Griswold v. Connecticut* expounded upon this. Unfortunately, what we have seen is a retrenching on the Fourth Amendment through a long period of time, both with respect to the government, with surveillance powers massively expanded with the Patriot Act, with renewed efforts to do that with ill-conceived ideas like the Corporate Transparency Act.

And then we have seen, really over the past 30 years, as technology has gone around, most of the billionaires in Silicon Valley and, frankly, Mr. Bloomberg, have accumulated their wealth by monetizing data. It is quite valuable. In fact, it is more valuable than financial transactions. We do have a small segment carved out by Gramm-Leach-Bliley, but we are seeing even more fragmented. We have different standards that apply to different entities.

When a bank collects credit card data, for example, we see different things than, say, Google Pay. One of my colleagues, a Member who gives great advice to me, recently pointed out that he purchased an airline ticket using Google's product Chrome. And Google, being the great customer service entity that it is, decided that they should store that credit card information in Google Pay. It had nothing to do with Google Pay he had no intention of signing up for Google Pay. It is all just part of the great customer experience.

And I am sure that is in the fine print somewhere—I don't know how many pages or words are contained in Google's documents or how many times they are updated. I am sure we have all read them, right, printed them out, and checked each phrase before we clicked, "accept." And we can all take solace that when they went public, they promised not to be evil, right? But we see the other thing. They are going to monetize.

So when we talk about data minimization, Mr. Cardinal, you spoke of data minimization. You could minimize your data or at least attempt to. I only meant to share this with the airline, my credit card, when I entered it; or I only meant to share my health records with my health provider, yet Google has found a way to sell it.

Going down the panel, do people believe consumers should have to give consent for transference of that data to third parties? Just yes or no, please?

Ms. SAUNDERS. It should not happen. It should not happen in ways consumers would not expect. If you didn't expect Google to keep your credit card, they just shouldn't do it.

Mr. DAVIDSON. Thank you.

Mr. KAMARA. I think that would be the minimum standard, yes.

Mr. DAVIDSON. Thank you.

Mr. GILLIARD. Absolutely minimum standard.

Mr. DAVIDSON. Thank you.

Mr. CARDINAL. Someone has to consent.

Mr. DAVIDSON. Thank you.

Mr. POZZA. I think, taking out the aspect of a specific company, that there is—the consumer cannot be deceived under current law about what is going on with the data, and then if you are thinking about approaching it from, are you going to—

Mr. DAVIDSON. So they can't lie, cheat or steal, or deceive them. Right now, the problem is no one really enforces it, right? Google promised they weren't going to track you with their location services; and in theory, since they said they weren't going to do that in their terms of service, there would be a way to do it. The reality is that they are so sophisticated, the average consumer can't know whether they have stopped doing it, and the regulator right now would be the Federal Trade Commission, and they clearly do not have a way to monitor whether the companies are complying with the terms of service.

In the financial sector, we have regulators that do that. And at subsequent hearings, I would hope to get to who should actually oversee the regulatory framework in the United States of America, because conformance is not going to happen in the stated nature. It leads towards decay and abuse, unfortunately, and it is way past time for us to update our laws.

My time has expired, and I yield back.

Chairman LYNCH. I thank the gentleman. The gentleman yields back.

It is my pleasure to recognize the gentlewoman from Michigan, Ms. Tlaib, for 5 minutes.

Ms. TLAIB. Thank you, Mr. Chairman.

There are going to be very few times that you will see a lot of us agree, especially on issues that are so critically important to civil liberties, civil rights issues, but in this particular issue, I think you can find a lot of bipartisan support about the great concern in protecting our residents at home, their privacy, and so forth.

I want to kind of take this in a little different direction. I don't know how many of you all know, in Detroit, there is over \$1 million spending on a facial scanning system called Project Green Light, which enables police to identify and track residents, capturing hundreds of private and public surveillance cameras installed at parks, schools, health centers, gas stations, women's clinics, fast food restaurants, and even addiction treatment centers. It has been expanded to also even include churches and low-income housing.

Overall, this aggressive City-wide surveillance system has reached more than 500 of our City's businesses and institutions and community organizations.

Ms. Saunders, are citizens even aware that they are being recorded and that their images are being captured?

Ms. SAUNDERS. No, I am sure that they are not.

Ms. TLAIB. What are some of the implications of this technology being used in low-income housing specifically?

Ms. SAUNDERS. This is not an area of our expertise, but I am sure people would be concerned to know that they are being tracked and that their individual identities are in government databases being used in ways that they wouldn't expect.

Ms. TLAIB. Dr. Gilliard, do you have anything to comment about this?

Mr. GILLIARD. I do. I think particularly for marginalized populations, this is especially onerous, because they are already subject to lots of surveillance in their daily lives that they are not able to escape. They don't have the means either to avoid this kind of surveillance, but also, maybe there are questions of if they are on public assistance, have they had run-ins with law enforcement, things like that. And that level of scrutiny on anyone is harmful, but I think the physical, emotional, and psychological effects on people to think that they are constantly being watched or to know that they are constantly being watched, I think is very pernicious.

Ms. TLAIB. These are for-profit entities coming to sell to cities like Detroit, and other communities of color, technology that hasn't even been tested properly, and is flawed. Studies over and over again have shown that it is flawed. I think the ACLU even did a sample of Members of Congress, and I believe they misidentified the majority of the folks who are in there, especially the Brown/Black Members within the United States Congress.

Given that Black men, and boys especially, are already more than twice as likely to die in an encounter at the hands of police, there are really strong implications of what this would mean, but also the fact that these are low-income families, people who are being surveilled.

One of my residents told me the green light that flashes—they actually put a green light outside of their building. And when I asked the mayor about this, he said, "What do you mean?" I said, no, just you are telling this person that they are unsafe. You are letting the world know, as people are passing by, don't come here. It is unsafe. It is very counterproductive to trying to make people feel safe. It is saying, if you are poor, you deserve to feel less safe and to have kind of the stigma to be on you for living in public housing.

Currently, my colleagues, Representative Ayanna Pressley and Representative Yvette Clarke, and I introduced the No Biometric Barriers to Housing Act, which would prohibit completely any use of real facial recognition technology in Federal housing.

What would you all feel, is this something that you all would be able to support?

Mr. GILLIARD. Absolutely. I think more surveillance does not equal more safety. I think imperfect surveillance is bad, but perhaps perfect surveillance is even worse.

Mr. KAMARA. Yes, absolutely. Biometric data is very intrusive. It is very difficult to store and protect. If it gets leaked, if there is a data breach, biometric data is very hard to revoke. So, that is another issue. And a lot of these surveillance databases are connected with DMV data. They are connected with other datasets as well. There are also a lot of problems with, if you end up in one of these databases, it is very difficult to get off of it. That is another issue as well. So, absolutely.

Ms. SAUNDERS. That particular bill is a bit outside our organizational expertise, but as a general matter, we certainly are concerned about the collection of personal data about people without their consent, and also especially about data that may be used differently against different populations. And, as you note, there could be mistakes, especially if you don't test it for how it works for people of—

Ms. TLAI. No, there are actually documented mistakes.

I know I am out of time, but thank you, Mr. Chairman.

And thank you all so much for being here to testify.

Chairman LYNCH. Very insightful observations. Thank you.

The gentleman from Wisconsin, Mr. Steil, is recognized for 5 minutes.

Mr. STEIL. Thank you very much, Mr. Chairman.

Mr. Pozza, I would like to dive into some of your testimony. The European Union's General Data Protection Regulation gives individuals the right to be forgotten. This is kind of intuitive as to what this might mean as it relates to Facebook, and maybe as it relates to Google. I think where some of the struggle comes in is, in particular, financial services products, loans, and insurance. I can think of a life insurance product where that is very challenging, if somebody comes in and asks for the right to be forgotten, but they are the beneficiary of someone else's life insurance product. It gets a bit complicated.

Could you comment and provide some insight as to how the right to be forgotten and other digital deletions impact common financial products? And then, what other implications should policymakers be thinking of in this context?

Mr. POZZA. I think that is a great question. I think that the deletion right, as it is sort of known under California, or the right to be forgotten, needs to be assessed in a way that is contextual. The examples that you point out are the kinds of things that maybe under California's law could be business exemptions, right? So, it can't just be a broad brush. You should be able to delete your data in a way that the business can no longer function, or it needs it to use for other sorts of analytical tools to make sure that it is not discriminating or something like that.

There are lots of reasons why you would need to cabin something like that to be practical in terms of business. And I think that goes to just the general approach of being sensitive to the business concerns when making and creating these sorts of rights.

The second piece of this is, the ABA recently released a report—it is in my testimony—that talks about the way that these deletion rights might impact sort of data models that would then be incomplete if they're used for things like fraud detection. So, again, you could potentially have something in the law that carves out these

uses where it makes sense to make sure that companies have robust access to these datasets so they can use things like detecting fraud.

Mr. STEIL. Let me dig in here for a second. In particular, as it relates to this, where sometimes you have these conflicting regulations, where you are trying to work in multiple jurisdictions, and businesses and consumers, I think, face increasingly complicated sets of overlapping and conflicting rules. As you mentioned in your testimony, GDPR affects us since many of the services we are using are offered in Europe. CCPA, as you noted, is sometimes overlapping on this.

Could you comment how the complexity impacts businesses and consumers and how Congress should respond to the costly and complicated overlapping system of regulations?

Mr. POZZA. I think it is clearly costly for businesses, as I have talked about, to have multiple different regimes governing different kinds of data. I would also reiterate that I think it is difficult for consumers to have these different regimes because they don't necessarily have clear expectations about how their data will be treated, which is a lot of what we talked about today.

When it comes to looking at something possibly on a Federal level, I think the U.S. Chamber has some pretty good principles they have outlined that talk about things like a risk-based approach and being sort of technology-neutral as much as possible and realizing that there are these tradeoffs, that consumer control of their information clearly is an important value, and that there are other sorts of things, as you point out, where it intersects with other kinds of regulations that you just sort of need to balance those.

Mr. STEIL. I appreciate your time and testimony today.

Mr. Chairman, I yield back.

Chairman LYNCH. The gentleman yields back.

First of all, I would like to thank our witnesses for your testimony today and for helping the task force with its work.

Without objection, the following documents will be submitted for the record. We have received submissions from the American Bankers Association, the Electronic Transaction Association, Fidelity Investments, Finicity, Public Knowledge, and Plaid, P-l-a-i-d.

The Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

I wish you all a very happy and safe Thanksgiving. This hearing is now adjourned.

[Whereupon, at 11:00 a.m., the hearing was adjourned.]

A P P E N D I X

November 21, 2019

**Testimony to the House Committee on Financial Services Task Force on Financial Technology
Hearing: "Banking on Your Data: The Role of Big Data in Financial Services"**

November 21, 2019

Submitted by Don Cardinal

Managing Director, Financial Data Exchange

Chairman Lynch, Ranking Member Emmer, and Members of the Task Force; thank you for the opportunity to offer testimony at this important hearing. My name is Don Cardinal and I serve as the managing Director of the Financial Data Exchange, commonly known as FDX.

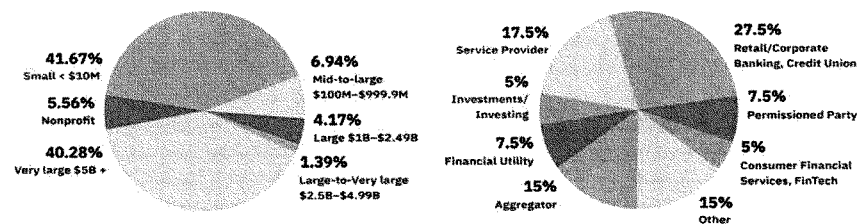
The mission of FDX is to unify the financial industry around a common, interoperable, royalty-free standard for secure and convenient consumer and business access to their financial data.

"Further coordination among all of the stakeholders in [data sharing] – 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."

– Center for Financial Services Innovation (CFSI) - Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration, Oct. 2016

FDX was founded by a group of the most innovative companies and engaged individuals operating in the financial services ecosystem and engaged in consumer permissioned financial data access. Collectively, the members represent over \$2 trillion (and growing) in market capitalization that includes major financial institutions, financial technology (fintech) companies, a consumer group and major industry groups, with continuous recruitment efforts to expand consumer group participation and consumer outreach. FDX members have in-depth experience in consumer permissioned data-sharing organizations that include key positions related to industry efforts, developing market solutions and providing input to regulators and lawmakers.

FDX Members



FDX marks the formation of the most comprehensive industry ecosystem to address the common challenges of consumer-permissioned data sharing. FDX seeks, through the development and promotion of a common standard, to facilitate the secure exchange of information, and accelerate innovation while giving consumers greater control of their data and better awareness of how it is being used.

FDX had its origins in early 2017 as a grassroots effort of financial institutions, financial technology companies and data aggregators seeking to find common ground for a secure, consumer-focused data sharing framework. Recognizing the significant progress already made by FS-ISAC's Aggregation Working Group in the 2015-2017 time period with its Durable Data Application Programming Interface (DDA) standard, FDX became a wholly owned, independent subsidiary of FS-ISAC¹ in 2018. FS-ISAC assigned the DDA (now known as the FDX API)² standard to FDX in October 2018 in connection with FDX's launch. As a non-profit organization, FDX will implement and oversee this interoperable standard and operating framework, continuing the development, improvement and adoption of the FDX framework.

To achieve its mission, FDX will focus on five (5) core operating principles of providing consumers and businesses: Control, Access, Transparency, Traceability and Security. The FDX framework will additionally adopt, reference or define:

- Standards for financial data sharing;
- Standards for secure authentication and authorization;
- A certification program and standards body; and
- User experience, consent guidelines and best practices.

FDX is comprised of committees and working groups focused on the mission of the organization, the promoting of the adoption of the FDX API standard and ensuring interoperability. Membership in FDX is broadly open to (in addition to Financial Data Parties (as hereafter defined) individuals, non-profits and groups (consumer and industry) with an interest in furthering the mission and objectives of FDX as described herein. We encourage all members to join working groups and participate at FDX events so that the voices of all interested members can be heard and contribute to the successful and broad adoption of the FDX API standard. Members are encouraged to adopt and promote the standards released by FDX. FDX anticipates that once its certification programs and procedures are established, widespread adoption of the FDX API as the industry standard will benefit consumers through consistent standards across platforms related to control, access, transparency, traceability and security of their financial data.

¹ Financial Services Information Sharing and Analysis Center (FS-ISAC) is an industry consortium dedicated to reducing cyber-risk in the global financial system. Serving financial institutions around the globe and in turn their customers, FS-ISAC leverages its intelligence platform, resiliency resources and a trusted peer-to-peer network of experts to anticipate, mitigate and respond to cyber threats.

² See "The ABC's of APIs" by visiting the FDX website at: www.financialdataexchange.org

FDX will promote royalty-free technology specifications – ensuring greater adoption – and will provide a certification program for parties wishing to mark their financial products and programs as compliant to FDX API standards.

Why FDX?

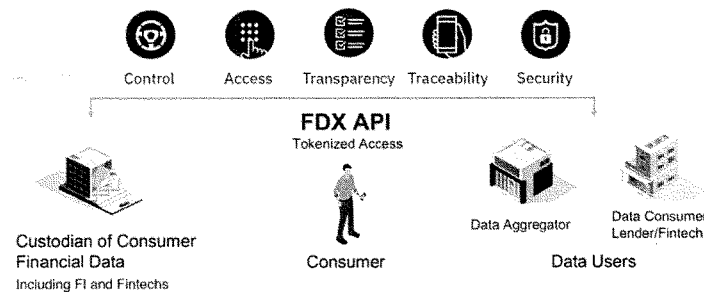
FDX was organized with the consumer in mind to ensure that the financial institutions, permissioned application providers/developers, financial data aggregators and other financial technology companies (collectively referred to herein as “Financial Data Parties”) can more readily and securely assist consumers in achieving their financial needs, better managing their finances and improving their financial health.

“Consumer-authorized access and use of consumer financial account data may enable the development of innovative and improved financial products and services, increase competition in financial markets, and empower consumers to take greater control of their financial lives. To accomplish these objectives, however, such access and use must be designed and implemented to serve and protect consumers.”

– Consumer Financial Protection Bureau, “Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation”, October 18, 2017

Consumers are increasingly utilizing online financial management services, payments, credit decisioning and more that are provided by companies that are often not affiliated with their primary financial institution (where consumer financial information is often located). To utilize these services, consumers need the ability to authorize access to their financial data from their financial institutions to other Financial Data Parties in a convenient, secure and reliable manner.

The Five Principles of Consumer-First Data Sharing



In order to give these parties access to their financial records, consumers have historically provided their login credentials (keys) to financial applications or data aggregators. In most cases, financial apps do not store the keys, but instead pass these credentials via an Application Programming Interface (API) to the data aggregator. The financial application or data aggregator can then access the financial institution website and retrieve the consumers' data (this process is known as screen scraping). While the consumer is granting rights to the financial application or to the data aggregator to use and store their keys, the use of APIs and token-based mechanisms for accessing data, as described herein, aims to eliminate the need to store keys and are generally seen as more secure and reliable. Implementing FDX's mission, objectives and operating principles on terms and conditions clearly understood and dictated by the consumer will address many of the concerns faced by consumers, industry and regulators today.

"During outreach meetings with Treasury, there was universal agreement among financial services companies, data aggregators, consumer fintech application providers, consumer advocates, and regulators that the sharing of login credentials constitutes a highly risky practice. APIs are a potentially more secure method of accessing financial account and transaction data than screen-scraping."

– U.S. Dept. of The Treasury, "A Financial System That Creates Economic Opportunities – Nonbank Financials, Fintech and Innovation" July 2018

In October 2016, the Center for Financial Services Innovation (CFSI) published a white paper that recommended all players come together to create standards for consumer data access. CFSI envisioned:

"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."

FDX believes in listening to all industry voices and coordinating with the various participants to benefit the consumer. An industry-led initiative such as FDX offers the shortest critical path to realizing the benefits of secure, consumer-permissioned data sharing.

Other industries have successfully created Special Interest Groups to address such industry challenges. The Bluetooth Special Interest Group and the Mortgage Industry Standards and Maintenance Organization (MISMO) are good examples of the voices of industry coming together to successfully create a common standard. FDX is another such example of multiple parties in an ecosystem coming together to form an organization singularly focused on a defined mission and established objectives.

FDX Mission and Objectives

“Treasury sees a need to remove legal and regulatory uncertainties currently holding back financial services companies and data aggregators from establishing data sharing agreements that effectively move firms away from screen-scraping to more secure and efficient methods of data access. Treasury believes that the U.S. market would be best served by a solution developed by the private sector, with appropriate involvement of federal and state financial regulators. A potential solution should address data sharing, security, and liability. Treasury recommends that any potential solution discussed in the prior recommendation address the standardization of data elements as part of improving consumers’ access to their data.”

– *U.S. Dept. of The Treasury, “A Financial System That Creates Economic Opportunities – Nonbank Financials, Fintech and Innovation” July 2018*

The mission of FDX is to unify the financial industry around a common, interoperable, royalty-free standard for secure and convenient consumer and business access to their financial data. Doing so will empower consumers to make information-based decisions on their personal finances and help increase financial literacy. FDX will accomplish its mission through execution of the following objectives:

- **Define Use Case Profiles:** FDX will define use case profiles describing consumer-permissioned scenarios within the financial data ecosystem. FDX will adopt and promote principles for data sharing across all use case profiles. Members will be able to qualify their solutions for one or more profiles.
- **Adopt, Promote and Improve Data-Sharing Standards:** FDX will develop and promote the FDX API standard and brand to help ensure financial data is timely, consistent, and accurate. Membership in FDX will allow use of and/or contribution to the specifications.
- **Adopt, Promote and Improve Secure Authentication Standards:** Consumers should not have to reveal their account login credentials to third parties to share financial data in the applications they choose. FDX will adopt modern standards in the FDX API specification in accordance with industry best practices with regard to authentication, authorization, data privacy and security in order to eventually do away with sharing login credentials with third parties to reduce risk to consumers.
- **Develop a Certification Program:** FDX will create a qualification and certification program to ensure common implementation and interoperability. Products (i.e., programs and apps for consumer-permissioned financial data sharing) will be approved by FDX through the certification program, to test the technical compatibility/interoperability, prior to being marketed as a compliant product, or getting access to certain intellectual property rights.
- **Develop User Experience and Consent Guidelines Best Practices:** FDX will document the steps and show examples of recommended user experiences across the end-to-end data sharing workflow to permit users to establish their financial data sharing connections with ease and full transparency and control. These steps will span across

the lifecycle of creating a connection, managing a connection, and revoking a connection, including the steps of disclosure, authentication and authorization.

- **Seek Broad Adoption of the FDX API Standard:** FDX will seek universal adoption of the FDX API standard. Significant adoption by financial industry participants will be required to realize the full benefit of establishing a unifying standard.
- **Future Applications:** Achieving FDX's mission and objectives through its operating principles and broad adoption of the FDX API standard may further support the development of a liability framework by the appropriate parties as encouraged by the U.S. Dept. of Treasury.

FDX Operating Principles

"Consumer Protection Principles [are] intended to reiterate the importance of consumer interests to all stakeholders in the developing market for services based on the consumer-authorized use of financial data. [These Principles include] ...Access..., Control and Informed Consent..., Security..., Access Transparency... and Efficient and Effective Accountability Mechanisms [Traceability]."

– *Consumer Financial Protection Bureau, "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation", October 18, 2017*

FDX believes accessible, consumer-permissioned financial data sharing not only enables consumers to better understand their financial situation, but also serves as a catalyst for innovation in the financial industry by seeking to:

- Empower consumers and organizations alike to leverage, and benefit from, their financial data.
- Facilitate access to financial data to improve financial literacy, financial decisions and convenience.
- Develop principles in concert with thought leaders in the financial industry as well as regulatory entities and worldwide standards bodies.

To ensure FDX always serves the best interests of consumers, its work and operations are based on five (5) core principles:

- 1.) **Control:** Consumers should be able to permission their financial data for services or applications.³
 - a. All Financial Data Parties should provide clear, intuitive navigation and information to consumers, allowing informed decision making on sharing financial data.

³ Members of FDX (and certain additional parties agreeing to FDX's Terms & Conditions) have access to FDX's "Control Considerations for Consumer Financial Account Aggregation Services" (Control Considerations). See Control Considerations: Overview – The Solution.

- b. Consumers should have the ability through easy, intuitive interfaces, to effortlessly grant, modify and revoke access to their financial data for applications or services they desire to use.
- 2.) **Access:** Account owners should have access to their data and the ability to determine which Financial Data Parties will have access to their data.
 - a. Intuitive navigation: The authentication process should avoid unnecessary steps or language that delays, interrupts, or impedes access.
 - b. Speed of access: Hand-off between parties and systems should be convenient, smooth, secure and efficient. Time-consuming or confusing experiences represent a barrier and frustrate consumers.
 - c. Responsible Access: Consumers should provide informed consent (with the ability to revoke that consent) for any and all access granted to Financial Data Parties. These parties will then only have access for the purposes for which the consent was provided.
- 3.) **Transparency:** Individuals using financial services should know how, when, and for what purpose their data is used. Only data that is required to provide such services should be shared with the organization providing the service.
 - a. Consumers should be able to view who they have permissioned, as outlined above in "Control."
 - b. When permissioning a new service, consumers should be fully informed regarding what their data is used for, how long the service can access that data, who it is used by, and under which terms the service is provided.
- 4.) **Traceability:** All data transfers should be traceable. Consumers should have a complete view of all Financial Data Parties that are involved in the data-sharing flow.
 - a. Data users (organizations and service providers) should know each step the data takes in order to permit the consumers to follow the path for each data flow. Data flows should be easily traceable and logged as the data traverses (i.e., from the financial institution through the aggregator and to the applications) in order to aid the pinpointing of potential errors or suspicious connections.⁴
 - b. Traceability may be used to support operational efficiencies and remediation activities. Additionally, it may also result in the faster detection and response to potential errors and suspicious traffic, as well as helping to pinpoint the source of the issue.
- 5.) **Security:** Financial Data Parties need to ensure the safety and privacy of data during access and transport and when that data is at rest.⁵
 - a. Financial Data Parties need to provide clear definitions on data usage and privacy, permitting consumers to make educated decisions.

⁴ See Control Considerations: Intermediary Identity – Benefits.

⁵ See Control Considerations: Aggregation and Security Guidelines.

- b. All parties involved in the data-sharing ecosystem must have appropriate security policies and practices in place. These practices should reflect best-in-class standards and be improved upon continuously.
- c. Security should empower consumer control, access, transparency, and traceability and should not be implemented in a manner that introduces friction points or other features that contravene these principles.

FDX fully expects all members to quickly move towards implementation that supports these core principles – and provides required support so all members are able to adopt them.

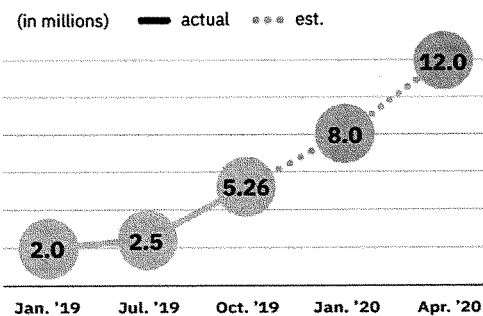
FDX Operations

FDX is working to align the financial industry around a single technology standard and solution qualification program that ensures “out of the box” interoperability. It will accomplish this through a technology organization structure similar to other technology initiatives that have successfully aligned other industries.

FDX’s four (4) primary activities are to:

- 1.) Publish data and authentication standards, specifications, and best practices for defined use cases;
- 2.) Evangelize the FDX API standard and promote and enable rapid adoption of the standard;
- 3.) Protect FDX trademarks and intellectual property while ensuring the specifications remain royalty free; and,
- 4.) Administer the qualification and certification program.

U.S. Customers on the FDX API



Committees and Working Groups

The FDX board of directors is comprised of financial institutions, financial technology companies, data aggregators and permissioned parties. The board, along with all FDX members, works diligently to continue to develop and improve the FDX API. In order to engage the participants in an ecosystem that represents multiple voices in the industry, FDX created several committees and working groups with active and ongoing participation from member organizations.⁶

- 1.) **Technical Review Committee**: tasked with the ongoing maintenance and improvement of the FDX API technical specification, along with adopting or building other technical solutions to promote FDX objectives. The Technical Review Committee oversees several working groups to achieve these goals.
- 2.) **APIs/Data Structures Working Group**: tasked with creating programs and processes that will certify proper implementation of the FDX API standard, ensuring interoperability.
- 3.) **Security & Authentication Working Group**: tasked with the design of appropriate security and authentication protocols and related matters.
- 4.) **Marketing and Public Relations Working Group and Government Affairs Task Force**: responsible for membership, marketing, government outreach, public relations and event planning.
- 5.) **User Experience/Consent Working Group**: focused on best practices for user experience, consent matters and user engagement. The working group will work closely with the Consumer Advocacy Working Group in order to improve standards, specifications, best practices relating to the consumer experience.
- 6.) **Open Financial Exchange**: As of July 2019, OFX has joined FDX as a working group to enable development of a unified standard. The independent working group is tasked with maintaining and evolving the OFX standard as necessary to support the existing OFX implementations, while leveraging the use cases and work between the OFX and FDX standards and providing a migration path to FDX for OFX users wishing to migrate.
- 7.) **Consumer Advocacy Working Group**: composed of non-profit consumer advocacy groups who will elect from among themselves a board level observer. The consumer advocacy members will provide input and recommendations at the working group and board level to ensure that consumer needs, security, experiences and rights are kept at the forefront of FDX's decision making process.

Comparison with Other Industry Forums

FDX's mission and approach is unique to any existing financial industry forum. With its focus on creating an interoperable standard by financial use case, it expects to adopt or extend existing standards and innovate new ones to accomplish its objectives. FDX is the first industry group with a broad range of support and active membership by major industry participants: financial institutions, permissioned application providers, financial technology companies, financial

⁶ Members of FDX may request a copy of the Charter Documents for each of the Working Groups referenced herein.

industry groups, data aggregators and consumer groups. Despite the size of many of its members, FDX is open to nonprofits and consumer groups (at discounted rates) and individual industry participants. FDX was founded with benefits to the consumer in mind. The protection and ease of permissioned sharing of consumers' financial data through the adoption of a common, interoperable, royalty-free standard for secure and convenient consumer and business access to their financial data remains FDX's top priority.

**PREPARED TESTIMONY AND STATEMENT FOR THE RECORD
OF**

Christopher Gilliard, PhD

HEARING ON

“Banking on Your Data: the Role of Big Data in Financial Services”

BEFORE THE

House Financial Services Committee

Task Force on Financial Technology

My name is Dr. Chris Gilliard, and I have spent the last 6 years studying, teaching, and writing about digital privacy and surveillance. I focus on the ways that digital technologies perpetuate and amplify historical systems of discrimination. Too often, digital technology renders systems invisible and inscrutable under the guise of proprietary code, black box algorithms or Artificial Intelligence. There are now countless documented examples of algorithmic discrimination¹, data breaches, violation of consumer privacy², and extractive practices on the part of platforms.³ At present, the de facto ethic of "move fast and break things" operating under codewords like innovation and disruption—and in an environment where the few existing regulations are seldom enforced—companies have been able to use consumer data in whatever ways serve the financial interest of the corporation. Moving forward, the onus for addressing these problems must be shifted onto companies, so that before they move their product to market, they provide evidence that they will not bring harm to the consumer, much in the same way food and drug safety operate now.

When we think about how Big Data operates in the financial marketplace now, it may not be possible or useful to define the distinction between "financial big data" and all other data. Financial "big data" plays a role not only in Finance, Insurance, Real Estate, but also in employment, transportation, education, retail, and medicine. Because the market does not make that distinction, we cannot either. In addition, third party data brokers accumulate all manner of data, to the point that even if there are categories of data that are protected,

¹For more information, see Safiya Noble, *Algorithms of Oppression* (2018); Virginia Eubanks, *Automating Inequality* (2018)

² See Carole Cadwalladr's work on Facebook and Cambridge Analytica
<https://www.theguardian.com/news/series/cambridge-analytica-files>

³ For more information, see Shoshana Zuboff, *Surveillance Capitalism* (2018)

processing massive amounts of data often creates the existence of proxies that allow for discrimination against protected classes within or among systems that may not appear to be "financial." For example, Cracked Labs reports that "Oracle claims to have data on billions of purchase transactions from 1500 leading retailers." ⁴

The primary reasons that many people remain unbanked are because of historical inequality. While new forms of banking and credit may provide access to systems those people have traditionally not had access to, many of these technologies also offer these benefits in exchange for people's privacy or create opaque systems that offer consumers little opportunity for redress. It is telling that the Apple Goldman Sachs card⁵ received so much interest, because opaque algorithms affect marginalized populations all the time, yet they do not have the reach and power to trigger massive media attention and an investigation by the state. Yet the stakes could not be any more different. For rich folks, it may mean being denied a larger credit limit; for the poor this may mean paying for medicine, shelter or food.

The notion that companies like Facebook, Google, Amazon are entering into banking in order to benefit the unbanked or people who do not have access to traditional credit markets is absurd on its face. As one recent report in Bloomberg asserted, regarding Google's proposal to partner with banks to offer checking accounts through its Google Pay

⁴ https://crackedlabs.org/dl/CrackedLabs_Christi_CorporateSurveillance.pdf

⁵ For more information, see <https://www.washingtonpost.com/business/2019/11/11/apple-card-algorithm-sparks-gender-bias-allegations-against-goldman-sachs/>

Testimony of Christopher Gilliard

"Banking on Your Data"

app⁶. "For Google, the bank partnerships will give the tech behemoth a better ability to show advertisers how marketing dollars spent on its system can drive purchases..."

There are two crucial frameworks for understanding these technologies and their impacts on marginalized communities: digital redlining⁷ and predatory inclusion. Digital redlining is the creation and maintenance of technology practices that further entrench discriminatory practices against already marginalized groups—one example (among many) being when journalists at ProPublica⁸ uncovered the fact that Facebook Ad targeting could be used to prevent Black people from seeing ads for housing, despite the Fair Housing Act prohibiting such conduct.

Predatory inclusion is a term coined by scholars Louise Seamster and Raphaël Charron-Chénier to refer to a phenomenon whereby members of a marginalized group are offered access to a good, service, or opportunity from which they have historically been excluded but under conditions that jeopardize the benefits of access. "... the processes of predatory inclusion are often presented as providing marginalized individuals with opportunities for social and economic progress. In the long term, however, predatory inclusion reproduces inequality and insecurity for some while allowing already dominant social actors to derive significant profits."⁹ As an example of this, we might look at a report on the cash advance

⁶ Jennifer Surane <https://www.bloomberg.com/news/articles/2019-11-17/google-checking-accounts-may-give-banks-an-edge-in-deposit-wars>

⁷ Gilliard and Culik, "Digital Redlining, Access, and Privacy" <https://www.common-sense.org/education/articles/digital-redlining-access-and-privacy>

⁸ Angwin and Parris Jr. *Facebook Lets Advertisers Exclude Users by Race* <https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race>

⁹ *Predatory Inclusion and Education Debt: Rethinking the Racial Wealth Gap*, 4 Social Currents (2017)

Testimony of Christopher Gilliard

"Banking on Your Data"

app Earnin, which offers loans and users are able to "tip" the app. As reported in the *NY Post*, "If the service was deemed to be a loan, the \$9 tip suggested by Earnin for a \$100, one-week loan would amount to a 469 percent APR."¹⁰

As Princeton professor Ruha Benjamin has argued, "our starting assumption should be that automated systems will deepen inequality unless proven otherwise."¹¹

Because of how algorithms are created and trained, historical biases make their way into systems even when computational tools don't use identity markers as metrics for decision making, but because of preexisting social realities and also because of the ways that so many different data points can serve as proxies for prohibited categories. Further, the notions of consent, "notice and consent" or "informed consent" as they are currently constructed are not sufficient for a number of reasons: privacy policies mainly serve to protect companies; credit scoring companies operate w/o the express consent of the consumers they purportedly serve. (I cannot opt out of being a "customer" of Experian, Equifax, and Transunion for instance); data is extracted, collected, combined, processed and used in ways that go beyond the stated purpose provided to consumers; there is often limited accountability for when they have been irresponsible with consumer data; companies rarely disclose and consumers even more rarely understand the full range of uses for their data.

We must reject the notion that regulations stifle innovation, as those harmed during innovation phases tend to be the most marginalized, and only later are policies addressed

¹⁰ Kevin Dugan *Popular cash advance app Earnin operating in payday loan 'gray area,' critics claim* <https://nypost.com/2019/03/21/popular-cash-advance-app-earnin-operating-in-payday-loan-gray-area-critics-claim/>

¹¹ *Rework, a Podcast by Basecamp* <https://podcasts.apple.com/us/podcast/bonus-breaking-the-black-box/id1264193508?i=1000456947960>

Testimony of Christopher Gilliard

"Banking on Your Data"

with no repairing of harms. The idea that corporate innovation, rather than the rights of historically marginalized groups, is an interest that Congress must protect turns ideas of citizenship and civil rights upside-down. The typical life cycle of a technological harm is human decision making leads to a technical failure. That these systems are proprietary often make the harms more difficult to detect. Companies often offload the responsibility of detecting harms to researchers and journalists, and the companies then only correct the harm after their discrimination or failures have been pointed out, and even then grudgingly often not completely, and finally the entrenchment of the unregulated system is used as argument that there should be no further regulation.

While at the beginning of this document, I called for companies to provide evidence that their products first do no harm, this should not be mistaken as a call for companies to self regulate. This model is unsafe and unsustainable. Consumers need to be empowered, as do regulators, in order to provide an environment that fully protects individuals' rights.

Statement by Seny Kamara

Associate Professor
Department of Computer Science
Brown University

Chief Scientist
Aroki Systems

before the

Task Force on Financial Technology

of the

Committee on Financial Services
U.S. House of Representatives
November 21, 2019

Chairman Lynch, Ranking Member Emmer and distinguished members of the Task force on Financial Technology. I appreciate the opportunity to testify at today’s hearing on the role of big data in financial services. Today, I will speak about how data is transforming the financial industry and how this transformation holds great promise but—unless it is carefully guided—also has the potential to erode consumer privacy and increase discrimination.

Experience. I am an Associate Professor of Computer Science at Brown University, where I conduct research in cryptography: the mathematical science that underlies data privacy and security. I am an affiliate of the Brown Data Science Initiative and of the Brown Center for Human Rights and Humanitarian Studies. Prior to Brown, I was a research scientist at Microsoft Research working in the Cryptography Research group. Over the last 20 years, I have developed a number of encryption algorithms and cryptographic protocols for data protection and privacy.

Overview. The financial industry is being transformed by technology. Examples include mobile devices, the Internet of Things (IoT), blockchains, smart contracts and machine learning. Both traditional institutions and technology startups are leveraging these technologies to provide new financial services to consumers. These developments can provide great benefits to consumers. Benefits that include expanding credit to the underbanked, offering better insurance rates to homeowners and improving fraud detection. While I want to recognize

the importance of these outcomes, it is critical that consumers and lawmakers understand the tradeoffs that these new financial technologies require. As is often the case when technology “disrupts” an industry, Fintech has the potential to both improve and harm the lives of people. These harms include the erosion of privacy and new forms of “algorithmic” discriminatory and predatory practices.

How Big Data is used in Financial Services

Big data usually refers to massive datasets and the systems and algorithms used to store, manage and analyze them. The data we produce—and is produced about us—is expected to grow from 29 zettabytes in 2018 to 175 zettabytes in 2025 [3]. While most conversations about big data focus on its size, an important dimension of data that is often overlooked is its *type*.

Types of data. Data comes from a variety of sources and is produced for a variety of reasons. For the purposes of this discussion, I will characterize data into three categories. The first is *authored data* which is produced by people. This includes emails, messages, tweets, comments and documents. The second category is *observational data* which is data that is produced about people by third parties; be it other people or algorithms. This includes, for example, medical records produced by physicians, consumer credit data produced by lenders, location data produced by mobile devices and automotive data produced by IoT devices in cars. Finally, there is *meta data* which is data that describes other data; for example, the date and time a piece of data was created and who the author was. It is important to highlight that *all* these data types are sensitive, not only authored data. In fact, it is by now well understood in the privacy research community that “all data is personally identifiable information”. This is the case because even innocuous looking data about an individual can be correlated with her identity [9].

Data sources. The Financial industry is using new data sources, including authored, observational and meta data. These new sources, often called *alternative* data, range from utility bills to location data and text messages. For example, credit reporting agencies like Experian, TransUnion and Equifax are using data about “every day bills” to create new credit scores. Insurance companies and startups are using IoT data from homes and cars to better predict risk. In the past, some insurance startups tried to use Facebook posts and psychometric tests to assess people’s risk profile [6]. Some mobile lending apps track location to determine how much time their users spend at work [2]. New micro-lending apps are using location data, social media content, contact lists and the behavior of Facebook friends to estimate people’s credit-worthiness. An app made in California that operates in Kenya, even accesses call history under the belief that people who regularly call their mothers are more likely to repay their loans [5].

Collection and storage. Some of these Fintech apps have privacy policies that are vague and unfavorable to consumers. The data they collect is intrusive and sensitive and their terms of service effectively grant app developers ownership of customer data. Furthermore, data collection often occurs in the background even when the app is not in use and the collected data is stored and analyzed on company servers even after the app has been deleted [5].

Data processing. In addition to leveraging new sources of data, the financial technology industry is also processing data in new ways using machine learning models to make automated decisions quickly and at scale. While classical algorithms are designed by domain experts and expressed by a series of rules and explicit choices, machine learning models are produced by *algorithms* that learn from data. The models produced in this manner can be very effective in certain contexts but suffer from important limitations. The first is a lack of transparency: we often do not know and, therefore, cannot explain why a machine learning model makes a particular decision. This is a serious concern in the context of credit since the Equal Credit Opportunity Act (ECOA) and the Fair Credit Reporting Act (FCRA) require creditors to explain the reason an application was denied. The second important limitation of machine learning models is bias in decision making. While this kind of algorithmic discrimination has been well-publicized in the last few years, it is important to note that we are only in the very early stages of rigorously understanding this behavior of algorithms. In fact, in this space, there are currently more questions than answers so it is important to tread carefully. One thing we do know is that simply ignoring protected attributes like race and gender in machine learning is not enough to guarantee unbiased decisions [1] but some Fintech companies claim exactly this [11]. This is a serious concern in the context of the Equal Credit Opportunity Act and the Fair Housing Act, both of which prohibit discriminatory lending practices.

Privacy Laws and Financial Data

The privacy of financial records is governed by the Gramm-Leach-Bliley Act (GLBA), the Bank Secrecy Act, the Right to Financial Privacy Act and the FCRA. It is important to note, however, that these laws apply to financial records but that is not the entirety of the data a financial institution collects. Here, strong privacy laws like the California Consumer Protection Act (CCPA) fill an important gap left open by existing laws. Also, as new financial services and companies emerge, it may be difficult to ascertain whether they qualify as financial institutions as defined by pre-existing law. Filling this gap is critical and the Financial Information Data Modernization Act (FIDMA) clarifies uncertainties in the GLBA while providing strong protections for consumers with an eye towards to advances not only in financial technology but privacy technologies as well.

Innovations in Privacy Technologies

Fintech apps can make use of multiple sources of consumer data, ranging from financial records provided by a bank to location data provided by a mobile device. Traditionally, financial apps have shared data through a practice called *screen scraping*, where an app asks a user for their credentials (i.e., login and password) so that it can log into the user's accounts on its behalf and retrieve the information it needs. It is widely accepted that this practice is substandard from a privacy and security perspective since users have to completely trust the app to store, protect and not abuse its credentials.

APIs. A better approach, which is now being developed by the financial industry is to use APIs. Roughly speaking, APIs are standardized interfaces between apps that allow for easier inter-operability and improved security. With an API-based design, apps can access user data only through a user-approved token that determines which pieces of data can be accessed and for how long. APIs are a considerable improvement over screen scraping but they are far from enough to guarantee consumer privacy. With an API-based design, apps can still access, lose, exploit and abuse raw user data. And as long as consumers have to trust “data hungry” apps that scour their sensitive data under vague privacy policies, they will never have real privacy.

New privacy technologies. But what if consumers did not have to give up their data in order to benefit from financial and technological innovations? What if financial apps and services never had to see raw data? This might sound impossible but, in fact, it is! Over the last 30 years, cryptography researchers in academia and in industry labs have developed a wide array of cryptographic techniques to process encrypted data. This gives us the ability to run algorithms (including machine learning algorithms) over encrypted data, to search through encrypted files and to query encrypted databases—all without ever decrypting the data. This set of privacy technologies, which include secure multi-party computation, private set intersection, homomorphic encryption and encrypted search algorithms, can enable truly private data processing [4]. I want to stress here that these technologies are not science fiction; they are ready for use today. In fact, in 2017 the Boston Women's Workforce Council and Boston University deployed secure multi-party computation to privately analyze the wage gap in the greater Boston area [8]. This year, Google announced its deployment of private set intersection to privately process data with external partners [7]. And encrypted search algorithms are starting to be deployed by major database companies [10]. By leveraging these advances in cryptography, financial technologies could deliver on their promise to improve the financial health of their customers without them having to sacrifice their privacy.

The financial industry is being transformed by technology. And in the wake of this transformation it is easy to get carried away on a wave of technological optimism. As a computer

scientist, I believe in the power of technology but I am also acutely aware of its potential harms. As a cryptographer, I worry deeply about the erosion of privacy that these financial apps and services can cause. We are all aware of the constant occurrence of data breaches; of the weaponization of private data to micro-target people and affect their behaviors. Do we want another Equifax? Do we want another Cambridge Analytica? “Moving fast and breaking things” is not sound engineering practice and it is not sound policy. It is imperative that we proceed carefully and that we oversee this transformation with strong privacy laws and strong privacy technologies.

Thank you. I look forward to answering your questions.

References

- [1] Solon Barocas and Andrew Selbst. Big data’s disparate impact. *Calif. L. Rev.*, 104:671, 2016.
- [2] Branch. How does branch determine my advance limit? <https://support.branchapp.com/hc/en-us/articles/360029167251-Why-aren-t-my-hours-tracking->.
- [3] John Rydning David Reinsel, John Gantz. The digitization of the world from edge to core. *An IDC White Paper-#US44413318*, 2018.
- [4] Nigel Smart (ed), David Archer, Dan Bogdanov, Alexandra Boldyreva, Seny Kamara, Florian Kerschbaum, Yehuda Lindell, Steve Lu, Jesper Buus Nielsen, Rafail Ostrovsky, Jakob Pagter, Ahmad-Reza Sadeghi, and Adrian Waller. Future directions in computing on encrypted data, 2015.
- [5] Privacy International. Fintech: Privacy and identity in the new data-intensive financial sector, 2017.
- [6] Privacy International. Social media intelligence and profiling in the insurance industry: It’s not only the price you pay that will be affected. 2017.
- [7] Mihaela Ion, Ben Kreuter, Ahmet Erhan Nergiz, Sarvar Patel, Mariana Raykova, Shobhit Saxena, Karn Seth, David Shanahan, and Moti Yung. On deploying secure computing commercially: Private intersection-sum protocols and their business applications. *IACR Cryptology ePrint Archive*, 2019:723, 2019.
- [8] Andrei Lapets, Frederick Jansen, Kinan Dak Albab, Rawane Issa, Lucy Qin, Mayank Varia, and Azer Bestavros. Accessible privacy-preserving web-based data analysis for assessing and addressing economic inequalities. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*, page 48. ACM, 2018.

- [9] Arvind Narayanan and Vitaly Shmatikov. Robust de-anonymization of large sparse datasets. In *2008 IEEE Symposium on Security and Privacy (S&P 2008), 18-21 May 2008, Oakland, California, USA*, pages 111–125. IEEE Computer Society, 2008.
- [10] Lily Hay Newman. A plan to stop breaches with dead simple database encryption. *Wired*, 2019.
- [11] Tala. Data ethics & consumer protection. <https://tala.co/data-ethics/>.

Written Testimony of Duane Pozza
Partner, Wiley Rein LLP

Before the United States House Committee on Financial Services
Task Force on Financial Technology

Hearing entitled “Banking on Your Data: the Role of Big Data in Financial Services”

Thursday, November 21, 2019
Rayburn House Office Building, Room 2128

Chairman Lynch, Ranking Member Emmer, and Members of the Task Force on Financial Technology, thank you for the opportunity to appear today to discuss the role of big data in financial services.

I am a partner at Wiley Rein LLP, where my practice includes advising companies on the legal and regulatory framework for collecting, using, and managing consumer data, including in financial services. This includes counseling on U.S. and global data privacy laws, financial services laws and regulations, and emerging regulatory approaches and expectations around the use of artificial intelligence (AI) and machine learning technologies, which depend on large and sophisticated data sets. I previously worked at the Federal Trade Commission, including as an Assistant Director in the Division of Financial Practices in the Bureau of Consumer Protection. I helped organize the FTC FinTech Forum Series, which examined, among other things, the role of big data in financial services, including through a 2017 event that focused on the consumer-focused uses of artificial intelligence technology.¹

Data-driven financial services hold enormous potential to improve consumers’ financial lives. Companies can use consumer data responsibly to expand access to credit, provide customized financial advice, detect and prevent fraudulent behavior, and provide financial services at a lower cost. Companies are already using large and robust data sets to accomplish these objectives, and the development of machine learning and AI technologies will further advance what technology innovators can accomplish.

Companies using consumer data in innovative ways for financial decisions operate in an area with many significant laws and regulations on the books and multiple regulatory authorities. Companies must comply with well-established financial services laws, many of which implicate use of consumer data, as well as FTC guidance on data privacy and security. They must also comply, to varying degrees, with consumer privacy laws that reach across sectors, both on the international level (for example, the European Union’s General Data Protection Regulation) and state level (for example, the California Consumer Privacy Act). State laws in particular threaten to create a piecemeal compliance framework and burden businesses that already have substantial

¹ See *FinTech Forum: Artificial Intelligence and Blockchain*, FTC EVENTS CALENDAR (Mar. 9, 2017), <https://www.ftc.gov/news-events/events-calendar/2017/03/fintech-forum-blockchain-artificial-intelligence>.

compliance obligations. The experience with California’s law illustrates some of the challenges that companies face. As consumer data is increasingly used to provide better financial services, it is important to carefully consider consumer expectations and preferences around use of their information, and weigh the benefits that better financial services can bring and the significant cost of added regulation.

Using Consumer Data to Improve Financial Services

“Big Data” has no one definition. The National Institute of Standards and Technology (NIST) has defined big data in reference to the “Four Vs,” as “consist[ing] of extensive datasets primarily in the characteristics of volume, velocity, variety, and/or variability that require a scalable architecture for efficient storage, manipulation, and analysis.”² Each of these factors is important in how large data sets can be used effectively:

- (1) volume – the data sets are large and extensive;
- (2) velocity – data is generated, collected, and processed at a high rate, often in real time or near real time;
- (3) variety – different types of information can be used together in novel ways to draw inferences;
- (4) variability – this refers to changes in a data set, whether in the data flow rate, format/structure, or volume, that impacts its processing.

There has been widespread agreement that the use of big data “can produce tremendous benefits for society,” as the FTC noted in its 2016 report on big data.³ Large, sophisticated data sets can be used for a wide range of purposes in financial services. These range from purposes like fraud detection and compliance with anti-money laundering laws, to enabling better credit decisionmaking and providing consumers with financial management advice.⁴ At an FTC hearing last year on algorithms, artificial intelligence, and predictive analytics, panelists discussed, for example, use of big data analytics to arrive at “fraud scores” that can help predict whether a transaction request is from someone other than the card holder,⁵ as well as

² NATIONAL INSTITUTE FOR STANDARDS AND TECHNOLOGY, SPECIAL PUBLICATION 1500-1r2, NIST BIG DATA INTEROPERABILITY FRAMEWORK: VOLUME 1, DEFINITIONS 6, 11 (October 2019), *available at* <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-1r2.pdf>.

³ FEDERAL TRADE COMMISSION, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION (January 2016) at 2, *available at* <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf> (“FTC Big Data Report”).

⁴ For example, the FTC noted in its Big Data Report that “[c]ompanies have used big data to provide alternative ways to score populations that were previously deemed unscorable,” and that “big data algorithms could help reveal underlying disparities in traditional credit markets and help companies serve creditworthy consumers from any background.” FTC Big Data Report at 6-7.

⁵ FEDERAL TRADE COMMISSION, TRANSCRIPT OF SEVENTH HEARING ON THE COMPETITION AND CONSUMER PROTECTION ISSUES OF ALGORITHMS, ARTIFICIAL INTELLIGENCE, AND PREDICTIVE ANALYSIS, PRESENTATION OF MELISSA MCSHERRY, SVP, GLOBAL HEAD OF DATA PRODUCTS, VISA, (Nov. 13, 2018), *available at* https://www.ftc.gov/system/files/documents/public_events/1418693/ftc_hearings_session_7_transcript_day_1_11-13-18_0.pdf.

incorporation of new data sources into credit scoring.⁶ Moreover, while sometimes called “alternative” or “non-traditional” data, many of these data sets can consist of information that already exists but has not been available to be used at scale for certain purposes (such as the example of cash flow data in lending decisions, as discussed further below).

The use of advanced data for credit decisionmaking is particularly promising. Large data sets can enable lenders to better analyze credit risk, and potentially expand access to credit to those who find it difficult to obtain credit when evaluated using traditional credit models. Many consumers are “thin file” or “no file” consumers who lack an adequate credit history to generate a reliable credit score, and others have relatively low scores that do not accurately reflect their current level of creditworthiness.⁷

The non-profit FinRegLab recently released the results of a promising study that illustrates the ability of large-scale data analytics to responsibly expand access to credit without raising issues related to bias. FinRegLab analyzed data from six non-bank financial service providers that used cash-flow information as part of their credit decisionmaking. Cash flow data can be obtained from consumer or small business accounts, and has the advantages of the “four Vs” of big data: substantial volume and variety of transactions, updated constantly.

The organization’s study concluded that the “predictiveness of the cash-flow scores and attributes was generally at least as strong as the traditional credit scores and credit bureau attributes studied.”⁸ It also found that “participants appear to be serving substantial numbers of borrowers who may have historically faced constraints on their ability to access credit,” and in regard to fair lending, that “the degree to which the cash-flow data predicted credit risk appeared to be relatively consistent across subpopulations” of race, ethnicity, and gender, and “appeared to provide independent predictive value across all groups rather than acting as proxies for demographic group.”⁹ FinRegLab also found the use of cash-flow data for credit underwriting appears to be spreading more rapidly in small business lending than in consumer lending, and that it is being used not only by online lenders, but also banks, payment processors, e-commerce platforms, and accounting service providers to provide small business loans.¹⁰

⁶ FEDERAL TRADE COMMISSION, TRANSCRIPT OF SEVENTH HEARING ON THE COMPETITION AND CONSUMER PROTECTION ISSUES OF ALGORITHMS, ARTIFICIAL INTELLIGENCE, AND PREDICTIVE ANALYSIS, PRESENTATION OF ANGELA GRANGER, VP ANALYTICS, EXPERIAN 83 (Nov. 13, 2018), *available at* https://www.ftc.gov/system/files/documents/public_events/1418693/ftc_hearings_session_7_transcript_day_1_11-13-18_0.pdf.

⁷ The CFPB has estimated that “26 million Americans are credit invisible, meaning they have no credit history with a nationwide consumer reporting agency [and] [a]nother estimated 19 million consumers have a credit history that has gone stale, or is insufficient to produce a credit score under most scoring models.” Patrice Ficklin and Paul Watkins, *An update on credit access and the Bureau’s first No-Action Letter*, CONSUMER FINANCIAL PROTECTION BUREAU BLOG (Aug. 6, 2019), <https://www.consumerfinance.gov/about-us/blog/update-credit-access-and-no-action-letter/>.

⁸ *Fact Sheet: Cash-Flow Data In Credit Underwriting*, FINREGLAB, <https://finreglab.org/fact-sheet-cash-flow-data-in-credit-underwriting/> (last visited Nov. 18, 2019).

⁹ *Id.*

¹⁰ *Id.*

Top officials at the Consumer Financial Protection Bureau (CFPB) also recently announced the results of the Bureau's data analysis conducted in connection with its no-action letter to Upstart Network, Inc. ("Upstart"). Upstart's underwriting model uses traditional underwriting data and various categories of alternative data, including information related to borrowers' education and employment history, and also uses machine learning in making credit underwriting and pricing decisions. The CFPB findings illustrate the benefits of using large data sets and machine learning to responsibly expand access to credit. In particular, the agency found:

- The company's tested model approved 27% more applicants than the traditional model, and yielded 16% lower average APRs for approved loans.
- This expansion of credit access reflected in the results occurred across all tested race, ethnicity, and sex segments, resulting in the tested model increasing acceptance rates by 23-29% and decreasing average APRs by 15-17%.
- In many consumer segments, the results showed that the tested model significantly expanded access to credit compared to the traditional model.
- As for fair lending concerns, when comparing the tested model with the traditional model, the approval rate and APR analysis results provided for minority, female, and 62 and older applicants showed no disparities that the CFPB found to require further fair lending analysis under the company's compliance plan.¹¹

Regulatory landscape

Companies seeking to use large consumer data sets in financial services are currently subject to extensive regulation that governs how they deal with consumer data. Applicable federal laws include the Fair Credit Reporting Act (FCRA), Equal Credit Opportunity Act (ECOA), Gramm-Leach-Bliley Act (GLBA), and FTC guidance around data privacy and security. While the application of these laws may raise novel questions in some circumstances involving big data, and there may be opportunities to update or modernize them, financial services companies are already building in compliance as the volume and complexity of consumer data scale up.

FCRA. The FCRA, among other things, imposes obligations on consumer reporting agencies ("CRAs") that compile and sell defined "consumer reports" for purposes that include credit determinations. The FCRA requires CRAs to implement reasonable procedures to ensure "maximum possible accuracy" of consumer reports.¹² If a consumer files a dispute with a CRA, it must conduct a "reasonable investigation" as to the accuracy of the investigation.¹³ And when creditors make certain adverse decisions based on consumer report information provided by a CRA, the creditor must provide notice to the consumer and information about the CRA that provided the consumer report.¹⁴ In the context of big data, the FTC has said that "if an unaffiliated firm regularly evaluates companies' own data and provides the evaluations to the

¹¹ Ficklin and Watkins, *supra* note 7.

¹² 15 U.S.C. § 1681e.

¹³ *Id.* § 1681i.

¹⁴ *Id.* § 1681m.

companies for eligibility determinations, the unaffiliated firm would likely be acting as a CRA, each company would likely be a user of consumer reports, and all of these entities would be subject to Commission enforcement under the FCRA.”¹⁵

ECOA. The ECOA prohibits discrimination on the basis of race, color, religion, national origin, sex, marital status, age, or receipt of public assistance.¹⁶ In its Big Data Report, the FTC noted that ECOA applies to the use of big data analytics as well. So, for example, the report indicates that, in the FTC’s view, “if a company makes credit decisions based on zip codes, it may be violating ECOA if the decisions have a disparate impact on a protected class and are not justified by a legitimate business necessity.”¹⁷ Additionally, when a creditor takes an adverse action, it must provide a consumer notification that includes an explanation of the reason for a decision.¹⁸ The CFPB is also currently considering implementation of Section 1071 of the Dodd-Frank Act, which requires financial institutions to compile, maintain, and submit to the Bureau certain information concerning credit applications by women-owned, minority-owned, and small businesses.¹⁹

GLBA. The GLBA and its implementing regulations govern financial institutions’ treatment of consumer data in connection with certain products or services.²⁰ The CFPB’s implementing Regulation P, for example, requires covered financial institutions to provide certain privacy notices and to comply with certain limitations on the disclosure of nonpublic personal information to nonaffiliated third parties, and it requires financial institutions and others to comply with certain limitations on redisclosure and reuse.²¹ The FTC’s Safeguards Rule requires covered financial institutions to develop, implement, and maintain a comprehensive information security program, and the FTC is currently considering whether to amend the Rule to include more specific data security requirements.²²

FTC privacy and data security actions. The FTC brings enforcement actions to protect consumer privacy and data security under Section 5 of the FTC Act, and its jurisdiction extends to non-bank financial technology companies.²³ The agency has published industry guidance based on its enforcement actions. In the area of data security, for example, it has outlined expectations in its *Start with Security* publication and *Stick with Security* blog post series.²⁴

¹⁵ FTC Big Data Report at 15.

¹⁶ 15 U.S.C. § 1691 *et seq.*

¹⁷ The report further notes that, “[e]ven if evidence shows the decisions are justified by a business necessity, if there is a less discriminatory alternative, the decisions may still violate ECOA.” *Id.* at 19.

¹⁸ 12 C.F.R. § 1002.9.

¹⁹ See *CFPB Symposium: Section 1071 of the Dodd-Frank Act*, CFPB ARCHIVE OF PAST EVENTS (Nov. 13, 2019), <https://www.consumerfinance.gov/about-us/events/archive-past-events/cfpb-symposium-section-1071-dodd-frank-act/>.

²⁰ 15 U.S.C. § 6801 *et seq.*

²¹ See 12 C.F.R. Part 1016.

²² See 16 C.F.R. Part 314; Press Release, Federal Trade Commission, FTC Seeks Comment on Proposed Amendments to Safeguards and Privacy Rules (March 5, 2019), <https://www.ftc.gov/news-events/press-releases/2019/03/ftc-seeks-comment-proposed-amendments-safeguards-privacy-rules>.

²³ 15 U.S.C. § 45.

²⁴ See FEDERAL TRADE COMMISSION, *START WITH SECURITY: A GUIDE FOR BUSINESS* (June 2015) <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>; see also *Stick with*

New privacy laws

In addition to the existing laws, discussed above, that regulate how financial services companies can use large consumer data sets, new cross-sectoral privacy laws have been enacted. These include the EU's GDPR, as well as state laws like the CCPA. These laws have imposed additional compliance costs on financial services companies and have resulted in regulatory uncertainty around how to handle particular types of consumer data.

GDPR. The GDPR regulates the collection and processing of personal data for individuals located in the European Union, among other things. The GDPR is based on six core principles, including being lawful, fair, and transparent and limiting the storage of data.²⁵ Under these six principles, there are a number of rights that data controllers (and to a lesser degree, data processors) must honor, and well as other business obligations. The GDPR provides individuals with a number of rights, including rights of access, rectification, deletion, and data portability, and the right to restrict data processing.²⁶ The GDPR also requires purpose specifications for collecting and processing personal data, which functions as a potential limitation on the use of large data sets that might be utilized for purposes beyond which the data was originally obtained.²⁷ The GDPR additionally includes a "data minimization" principle that limits processing of personal data to what is "adequate," relevant," and "necessary" in relation to the purposes for which it is processed.²⁸ Even companies with relatively small European operations or customers have incurred significant costs in coming into compliance with GDPR.

CCPA. The California Consumer Privacy Act is the most significant privacy law enacted by a state so far. It goes into effect on January 1, 2020. The law applies to businesses that collect and control the processing of California residents' personal information, do business in the state, and meet certain qualifications in terms of revenues or data collection.²⁹ The "personal information" covered broadly includes traditional identifiers, commercial information, biometric information, unique personal identifiers (like IP addresses or cookies), internet information like browsing history or geolocation data, and inferences drawn from any information to create a profile about a consumer.³⁰

The law has created a number of compliance challenges for businesses. First, the substantive requirements of the law have been a moving target, and significant uncertainty remains about how to operationalize a complex and often unclear law, even though it will become effective in less than two months. Amendments to the law were passed and signed into law as late as October 11, 2019. On October 10, 2019, the California Attorney General released extensive

Security: A Business Blog Series, FTC BLOG (October 2017), <https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series>.

²⁵ See Eur. Par. And Council Regulation 2016/679 of Apr. 27, 2016 Protection of Natural Persons With Regard to the Processing of Personal Data and the Free Movement of Such Data, and repealing Directive 95/46/EC, art. 5 ("GDPR").

²⁶ See GDPR art. 15-18, 20.

²⁷ See GDPR art. 5(1)(b).

²⁸ See GDPR art. 5(1)(c).

²⁹ See California Consumer Privacy Act of 2018 ("CCPA"), Cal. Civ. Code § 1798.140(c) (2018).

³⁰ *Id.* § 1798.140(o).

draft regulations to implement the law, and many of these go beyond what is required in the law itself and are themselves ambiguous. Adding to the lack of clarity, we are in the middle of a two-month comment period regarding the draft regulations, which closes on December 6. The final regulations must be adopted by July 1, 2020. All of this creates a period of uncertainty and raises practical burdens for companies attempting to comply with the law. While enforcement of the law is delayed until July 1, 2020 or six months after the Attorney General adopts implementing regulations, companies are striving to put procedures in place for compliance by January 1 when the law goes into effect, but the specifics of many of the procedures governed by the draft regulations remain subject to change. Additionally, starting on January 1, covered consumers will be able to seek information about the collection of their personal information, and the disclosure or sale of their information to third parties that occurred over the past year.³¹ That means that, even now, before the law has gone into effect, we are in “look back” period where companies will have obligations for providing information about their use of personal information.

Second, the CCPA creates a patchwork of rules potentially applicable to financial institutions. Section 1798.145(e) states that the CCPA “shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act [GLBA] . . . and implementing regulations.”³² As noted above, however, the GLBA applies to defined “financial institutions” and covers only certain personal information that is provided by an individual, results from a transaction with or service performed for an individual, or is otherwise obtained by a financial institution, in connection with a financial product or service to be used primarily for personal, family, or household purposes.³³ As a result, some of the personal information that financial services providers collect, or collect for certain purposes, arguably may not be covered by GLBA and its implementing regulations and may be covered by the CCPA. Financial services providers may consider implementing new procedures – including notices and procedures for responding to and verifying consumer requests – that may apply only to certain data.

Third, the law imposes significant compliance burdens on companies that do business nationwide – while leaving open the possibility that other states could pass laws that go even further or that may be inconsistent with California’s mandates. This patchwork approach is confusing for both consumers and companies trying to comply with the law. These burdens will be felt by businesses of all sizes, and may be particularly problematic for small businesses, which may be covered because they deal with substantial amounts of consumer data.³⁴ Moreover, companies must build in compliance with the current law with an eye on what other state legislatures may pass in the near future.

Additionally, some observers have suggested that the CCPA may inhibit the ability to effectively collect and use large data sets for purposes of implementing machine learning models. A recent report by the American Bar Association Section of Antitrust notes that, if a significant number of

³¹ *Id.* § 1798.100(d).

³² *Id.* § 1798.145(e).

³³ *See* 15 U.S.C. § 6809(3), (4)(A), (9).

³⁴ Cal. Civ. Code § 1798.140(c)(1)(B).

consumers were to exercise their deletion rights in certain circumstances, that might result in data sets that are not representative of the relevant population.³⁵ The ABA report also raises the possibility that “it may be difficult for a company to specify at or before the point of collection the purposes for which the business will use the data in the context of analytics.”³⁶ Whether this proves true in practice, companies will want to think carefully about how they define the purposes for which they collect consumer data that may be incorporated into larger data sets to enable beneficial services to be provided to consumers.

+++++

Financial services companies are currently making significant advances in expanding financial services for the benefit of consumers. In evaluating current or proposed privacy laws in the context of “big data,” it is important to weigh any purported benefits against the significant benefits from innovation in financial services that consumers also want.³⁷ Particularly in financial services, we should recognize that new regulations have the potential to burden important pro-consumer innovation that can materially improve consumers’ financial lives.

Thank you again, and I look forward to answering your questions.

³⁵ AMERICAN BAR ASSOCIATION SECTION OF ANTITRUST, ARTIFICIAL INTELLIGENCE & MACHINE LEARNING: EMERGING LEGAL AND SELF-REGULATORY CONSIDERATIONS 59 (Sep. 30, 2019), *available at* https://www.americanbar.org/content/dam/aba/administrative/antitrust_law/comments/october-2019/clean-antitrust-ai-report-pt1-093019.pdf.

³⁶ *Id.* at 57.

³⁷ In the broader context of U.S. privacy law, the U.S. Chamber of Commerce has released privacy principles that can be found at https://www.uschamber.com/sites/default/files/9.6.18_us_chamber_-_ctec_privacy_principles.pdf.



**Testimony before the
U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON FINANCIAL SERVICES
Task Force on Financial Technology**

Regarding

“Banking on Your Data: The Role of Big Data in Financial Services”

November 21, 2019

Lauren Saunders
Associate Director

National Consumer Law Center
(on behalf of its low income clients)

1001 Connecticut Avenue, NW, Suite 510
Washington, DC 20036
202-595-7845
lsaunders@nclc.org

Testimony of Lauren Saunders, National Consumer Law Center
 Before the U.S. House of Representatives Committee on Financial Services
 Task Force on Financial Technology
 regarding
 “Banking on Your Data: The Role of Big Data in Financial Services”
 November 21, 2019

Summary

Chairman Lynch, Ranking Member Emmer, and Members of the Financial Technology Task Force, thank you for inviting me to testify today regarding the use of consumers’ data in financial services. I offer my testimony here on behalf of the low-income clients of the National Consumer Law Center.¹

Today I would like to focus on the rapidly growing use of data aggregators to access consumers’ bank account transaction and other account data in connection with a variety of financial products and services. Access to consumers’ account data has the potential to enable many products and services that may be beneficial to consumers, including use of cash flow data to improve access to affordable forms of credit, products that encourage savings, and a variety of services that help consumers better manage their finances.

At the same time, the intensely detailed and sensitive data inside consumers’ accounts can also be used for less beneficial purposes. It may help predatory lenders refine their ability to make and collect on unaffordable loans or allow consumers to be targeted for products that do not

¹ Since 1969, the nonprofit National Consumer Law Center® (NCLC®) has used its expertise in consumer law and energy policy to work for consumer justice and economic security for low-income and other disadvantaged people, including older adults, in the United States. NCLC’s expertise includes policy analysis and advocacy; consumer law and energy publications; litigation; expert witness services, and training and advice for advocates. NCLC works with nonprofit and legal services organizations, private attorneys, policymakers, and federal and state government and courts across the nation to stop exploitive practices, help financially stressed families build and retain wealth, and advance economic fairness.

improve their well-being. Transaction data can also be fed into algorithms or machine learning with results that lead to discriminatory impacts.

The use of data aggregators poses a number of questions and concerns regarding:

- Safe methods of accessing and storing data;
- Privacy, whether information is used in ways consumers would expect, and whether consumer choice and control are meaningful;
- Consumers' rights under the Fair Credit Reporting Act to know what information is being used, to demand accuracy, to obtain corrections, and to know when information results in adverse consequences; and
- Disparate impacts that result in discrimination against disadvantaged communities.

A number of efforts are underway to address many of these issues, including the work of Financial Data Exchange (FDX). While voluntary efforts by industry are welcome, ultimately consumers cannot have confidence that their data will be used in appropriate ways unless the law clearly protects them across these different dimensions. In particular, we support:

- Enhanced data security requirements for all entities, federal supervision of entities that store significant amounts of consumer data, and respect for consumer's right to contest unauthorized charges;
- A strong federal privacy law that does not preempt state privacy protections;
- Application of the FCRA to new forms of data access and collection;
- Disparate impact analysis for use of big data, enforcement of the Equal Credit Opportunity Act (ECOA), and protection against disparate impacts when data is used for purposes other than credit; and
- A greater role for the Consumer Financial Protection Bureau in supervising data aggregators for compliance with all applicable laws within its jurisdiction and enforcing privacy and data security standards.

A. Data Aggregators and the Use of Consumers' Account Data

In the past few years, data aggregators such as Plaid, Yodlee and Finicity have increasingly enabled companies, with consumer permission,² to access consumers' bank account, credit account, investment account and other account data in order to enable a growing variety of products and services.³ These data aggregators are not typically consumer-facing, but rather operate behind the scenes to provide other companies with information from consumer's financial accounts. Many of products and services offered by these financial technology ("fintech") and other companies show promise to benefit consumers. But uses of this data should be monitored, as there are many possible worrisome uses of and impacts of this data.

1. Credit scoring and cash-flow underwriting

Data aggregators, both directly and through partnerships with the big three credit reporting agencies, offer access to transaction data for purposes of underwriting credit. Transaction data may supply information that is not normally considered, such as utility or rent payments, or may be used to analyze the consumers' cash flow.

Some services, like ExperianBoost, may draw on bank account transaction data to enable lenders to consider a consumer's utility payments, which typically do not get included in traditional credit reports.⁴ Consumer-permissioned access to bank account transaction data is a better way to incorporate utility payment data than full-file utility reporting, which risks harming the scores of millions. Consumers who want creditors to consider their utility payments can grant access without pushing utility companies to report all payments for all consumers, which raises a host of

² But see section C below on the limits of consumer "permission."

³ For a discussion of some of the "fintech" companies that use data aggregators, see Lauren Saunders, National Consumer Law Center, *Fintech and Consumer Protection: A Snapshot* (March 2019), <http://bit.ly/2Tx9BmG>.

⁴ Susan Henson, Experian, *Introducing Experian Boost, a New Way to Instantly Improve Your Credit Scores*, April 8, 2019, <https://www.experian.com/blogs/ask-experian/introducing-experian-boost/>. Other services access certain utility, telecom and cable data from other sources, sometimes with consumer permission. See, e.g., Press Release, Equifax Continues Leadership In Alternative Data With Worldwide Urjanet Partnership Financial Information (Sept. 18, 2019), <https://investor.equifax.com/news-and-events/news/2019/09-18-2019-122941123>; FICO, FICO Score XD, <https://www.fico.com/en/products/fico-score-xd>.

issues including harmful impact on credit scores for many and interference with state utility shutoff protections.⁵

Other services incorporate the full range of bank account transaction data into credit scores or cash-flow underwriting. UltraFICO relies on bank account transaction information from Finicity, a data aggregator working in partnership with Experian.⁶ For now at least, UltraFICO will only be used to enhance a consumer's credit scores to see whether a denied application can be approved or a lower rate can be offered. A partnership between Equifax and Yodlee uses real-time bank account information like balances, deposits and withdrawals to augment other credit data. Some lenders, such as Petal, may also use data aggregators directly to access bank account transaction data.

Access to bank account transaction data can enable cash-flow underwriting, a potentially positive form of underwriting. Analysis of a consumer's actual inflows and outflows, income and expenses can be used alone or together with traditional credit reports to assess whether a consumer has the ability to repay credit.⁷ A look at the consumer's actual residual income may provide a realistic picture of whether the consumer regularly has sufficient funds at the end of the month to handle a loan payment or, conversely, whether the consumer has difficulty meeting expenses.

Cash-flow data may help those who do not have significant credit histories. Indeed, a CFPB study has speculated that that one of the primary "on ramps" to a credit report might be the consumer obtaining their first credit card from their own bank.⁸ The use of a data aggregator for

⁵ See, e.g., Letter from 40 associations, consumer, civil rights and advocacy groups to U. S. House of Representatives (Dec. 8, 2017), opposing H.R. 435, which would preempt state laws that do not permit utilities to submit payment information to credit bureaus, <https://www.nclc.org/images/pdf/legislation/letter-oppose-hr435-hfsc.pdf>; Comments of consumer groups in Response to Request for Information Regarding Use of Alternative Data and Modeling Techniques in the Credit Process, Docket No. CFPB-2017-0005, at 3 to 5 (May 19, 2017), https://www.nclc.org/images/pdf/credit_reports/comments-alt-data-may2017.pdf

⁶ FICO, Introducing UltraFICO, <https://www.fico.com/ultrafico/> (viewed July 21, 2019).

⁷ See FinRegLab, The Use of Cash-Flow Data in Underwriting Credit (July 2019), at 3 https://finreglab.org/wp-content/uploads/2019/07/FRL_Research-Report_Final.pdf (noting that cash-flow scores "frequently improved the ability to predict credit risk among borrowers that are scored by traditional systems as presenting similar risk of default").

⁸ Consumer Financial Protection Bureau, Data Point: Becoming Credit Visible, June 2017, https://files.consumerfinance.gov/f/documents/BecomingCreditVisible_Data_Point_Final.pdf, at 33 (noting that

account information allows this access even when a consumer does not have a deposit account at a large bank that also issues credit cards.

Analysis of transaction data may provide a way to underwrite consumers whose income comes from informal or irregular sources that is otherwise difficult to document. Transaction data can also substitute for more cumbersome methods of documenting income.

Cash-flow data may help consumers who are recovering from a temporary setback. Bank account data can avoid the need to rely on credit scores that reflect negative marks from economic hardships years ago.⁹ Data suggests that many of the consumers with impaired credit were the victims of unfortunate events such as illness or job loss.¹⁰ Bank account data can show when there has been a healthy sustained recovery from an economic shock such as a job loss or illness.

Today, most of these uses of cash-flow data only kick in to enhance a consumer's credit score in order to see if a consumer who was denied can be approved or if the consumer can be given a lower rate. They have the ability to help consumers without exposing them to the risk of lower credit scores or harming their existing credit report. Consumers also generally permission use of their data for a particular credit application.

However, with some services there are questions as to whether the consumer's opt in will allow ongoing use by any lender that accesses the service – or by the credit bureau more broadly – potentially in ways that the consumer does not expect or understand. It is also not clear that, as time goes on, all of these uses of cash-flow underwriting will only enhance a consumer's credit

"about 65 percent [of consumers studied], appear to have transitioned out of credit invisibility by opening an account by themselves despite their lack of a credit history" and that "perhaps some commercial banks are willing to lend to credit invisible consumers with whom they have existing deposit account relationships.")

⁹ Lenders often review 12 months of statements at most even when they manually review bank account activity. For example, Fannie Mae requires lenders to review 12 months of bank account statements to establish payment activity. Fannie Mae Selling Guide, B3-5.4-03: Documentation and Assessment of a Nontraditional Credit History, August 30, 2016, available at <https://www.fanniemae.com/content/guide/selling/b3/5.4/03.html>. Anecdotally, we have heard that some lenders only require 3 to 6 months of bank account statements.

¹⁰ About 70 to 80% of consumers with impaired credit or a low score, such as a 600, will actually not default. These may be victims of extraordinary life circumstances who do not default again once they have recovered economically. See Chi Chi Wu, NCLC, Solving the Credit Conundrum: Helping Consumers' Credit Records Impaired by the Foreclosure Crisis and Great Recession, Dec. 2013, at 9-11, available at www.nclc.org/images/pdf/credit_reports/report-credit-conundrum-2013.pdf (summarizing research).

score rather than decrease it. These broader uses of transaction data for credit underwriting bear monitoring, especially in light of the dismal record of the credit reporting agencies in being overly aggressive in selling the sensitive financial information of consumers.¹¹ The temptation to maximize the monetary value of this data will be significant.

2. Other uses of account transaction data.

Personal financial management services may use account transaction data to help consumers save or invest. Services can manage the inflows and outflows of consumers' accounts, identify when there are extra funds potentially available, and make it easy to transfer those funds to a savings or investment account.

Data aggregators can enable account verification when a consumer wishes to link an account for a person-to-person payment service, savings device, or other purpose. This linkage can be accomplished faster and easier than through older methods, such as using micro deposits that the consumer must wait for and then verify. Account data can also be used for identity verification in other contexts.

Other services allow consumers to better manage their money and identify or avoid bank fees. Some apps help consumers anticipate and cover upcoming bills or prevent or address overdrafts.¹² Other services consolidate bank, credit, investment, and other account information so that consumers can see the entire picture of their finances in one place.

Data aggregators can help companies provide competition for banks. Consumers can be a captive audience for banks, which have an edge over competitors due to the information they

¹¹ For example, the FTC spent many years battling TransUnion over its sale of target marketing lists. See *Trans Union Corp. v. F.T.C.*, 245 F.3d 809 (D.C. Cir. 2001) (upholding FTC's ruling and discussing history of the case). Consumer advocates have argued for many years that the practice of prescreening is nothing more than using consumer reports for marketing. See National Consumer Law Center, *Fair Credit Reporting* § 7.3.3 (9th ed. 2017), updated at www.nclc.org/library.

¹² I will not in this testimony address concerns about products that are offering credit in the guise of other services not covered by credit laws. See *Fintech and Consumer Protection*, *supra*.

hold on consumers. Data aggregators enable fintechs to reach consumers and compete, and also push banks to improve their own services.

Eventually, data aggregators may make it easier for consumers to close their bank account and transfer it elsewhere.¹³ Setting up bill payments for a variety of other accounts, redirecting preauthorized charges, and even collecting and storing transaction information can be a cumbersome process. The control that financial institutions have over account data and the difficulty of moving it elsewhere inhibit competition and lock consumers into accounts with which they are unhappy. Data aggregators might be able to help consumers easily transfer the data they need to a new account.

At the same time, not all of the potential uses of consumers' account transaction data are positive.

Enabling lenders to push more credit on consumers with subprime credit scores may not always be a good thing. It could instead lead people to become more overburdened by debt and in a worse position to manage their finances. Underwriting models that focus on the risk to the creditor are not the same thing as affordability by the consumer. Some lenders may access the timing and history of inflows and outflows from consumers' accounts to fine tune a predatory lenders' ability to collect but not necessarily the consumers' ability to afford credit. And for some purposes, credit invisibility could be better than a negative profile, such as a history of overdrafts, which could harm consumers in seeking employment and or in insurance pricing.¹⁴ Thus, we would advocate that account transaction data not be used for these purposes.

Some of the services offered through data aggregators may be mere pretenses to harvest consumer data that can be used for product pitches or other purposes. Companies may claim to

¹³ See Suzanne Martindale et al., Consumers Union, Trapped at the Bank: Removing Obstacles to Consumer Choice in Banking (May 30, 2012), <https://advocacy.consumerreports.org/wp-content/uploads/2013/09/TrappedAtTheBank1.pdf>.

¹⁴ See Testimony of Chi Chi Wu before the U.S. House of Representatives, Committee on Financial Services, Task Force on Financial Technology, regarding Examining the Use of Alternative Data in Underwriting and Credit Scoring to Expand Access to Credit (July 2019), https://www.nclc.org/images/pdf/credit_reports/testimony-alternative-data-credit-scoring.pdf.

be making offers in the consumers' best interest when they instead are motivated by advertising revenue or revenue sharing. Debt settlement products and others that frequently end up harming consumers finances could be pushed on consumers.

Consumers could eventually be required to provide access to their account data for use by employers, insurers, and other purposes not imagined today. Government agencies could even require "Big Brother" monitoring of purchases and spending as a condition for government benefits.

And, as discussed in section E below, account transaction data can also be used in ways that result in disparate impacts on vulnerable communities.

B. Data security and protection from unauthorized charges are critical.

Data security is obviously critical in any system that accesses or uses consumers' account data. Security issues are posed by the method of accessing that data; how the data is stored and shared; and how consumers are protected if there is a problem.

In the early days of account aggregation, access was typically gained by using the consumers' username and password to access the account (also known as "screen scraping"). More recently, many data aggregators have worked to strike agreements with financial institutions to access account data through secure automated programming interfaces (APIs). While APIs are a superior form of account access, bilateral agreements between individual data aggregators and individual financial institutions take time to negotiate.¹⁵ Screen scraping continues to be used if the consumer has an account at one of the vast number of financial institutions that do not yet have an API set up with the particular data aggregator. We support efforts to increase the use of

¹⁵ We are aware of concerns by data aggregators that financial institutions in these bilateral agreements may impose limits on the types or frequency of data that may be accessed. We take no position in these debates, but we do note, as discussed in section C below, that aggregators and the fintechs they work with should only access the minimum data needed, for the minimum amount of time, needed to perform the function that the consumer expects and authorizes.

APIs and eliminate screen scraping. Regulators may be able to play a role in facilitating these efforts.

Data security by both the data aggregator and the ultimate end user are also critical. The data aggregator may obtain the consumers' username and password even if an API is ultimately used, and the data accessed through account aggregation also is very sensitive and must be held securely. While data aggregators promise high levels of security, and many impose security requirements on end users, consumers have no capacity to evaluate the trustworthiness, security protocols, motives or activities of either data aggregators or the companies that offer services based on account data.

Even the largest banks with the most robust compliance regimes – that are subject to the data security rules of Graham Leach Bliley Act and are examined by the bank regulators -- have been subject to data breaches. Voluntary promises of data security by data aggregators are simply insufficient.

While consumers have legal protection against unauthorized charges, that does not mean that they will not be harmed by a data breach. Disputes about unauthorized charges can take time to resolve, depriving consumers of access to their funds in the meantime. Banks do not always believe consumers when they contest unauthorized charges. Data breaches can also harm consumers in other ways, such as by opening them up to potential identity theft for years into the future.

Congress must extend data security and privacy rules beyond the current scope of financial institutions under Gramm-Leach Bliley. It is also well past time to give federal regulators the authority and the mandate to begin regular data security examinations of consumer reporting agencies, data aggregators, and other companies that hold significant amounts of sensitive consumer data.

It is also critical that consumers' right to contest unauthorized charges – directly through their financial institution, not the data aggregator – be respected. In the past, some financial

institutions have taken the position that consumers lose their dispute rights and liability protection if they give a third party permission to access their account and unauthorized charges result. That is incorrect.¹⁶ Consumers still retain protection against unauthorized charges just as they would if they gave their debit card to their child who then is mugged. If the breach ultimately happened at the data aggregator or fintech end user, then the bank and data aggregator or other company can work out who should bear the ultimate liability. But with new data breaches happening every day, consumers have no way of knowing how an unauthorized charge happened. They must retain the right to go to the institution that holds the account to resolve the issue.

C. Privacy, consumer choice and control must be meaningful.

Beyond security risks, consumers also face privacy risks when they provide access to their account data. Consumers may believe that they are providing access only for purposes of a narrow range of transactions or services. But the third party can gain access to a wealth of information about the consumers' income, where they shop and what they buy, their spending patterns and a variety of other sensitive personal information. Some services harvest this information for marketing purposes and even at times may reserve the right to share it with or sell it to other parties that the consumer does not contemplate.

While data aggregators currently seek consumers' consent, consent alone does not provide consumers with sufficient protection. Today, people can easily choose to avoid products that require use of a data aggregator. But as the use of access to account information spreads, refusing to click "I agree" will become much harder, just as consumers do not truly have any power to say no if an employer wants to pull a credit report. Plus, if data gets incorporated into credit reports or is sold and resold, consumers may not even have the minimal control of providing consent for new uses.

¹⁶ See Comments of National Consumer Law Center (on behalf of its low income comments) in Response to Request for Information: Consumer Access to Financial Records, Docket No. CFPB-2016-0048 (Feb. 21, 2017), <https://www.nclc.org/images/pdf/rulemaking/comments-response-data-aggregator.pdf>.

Consent alone is also insufficient because the vague privacy policies that consumers receive do not give them any real idea of how their information may be used. Consumers should not be expected to decipher privacy policies to hunt for inappropriate uses. Consumers also may have used a service once or twice to try it out and long forgotten about it, not realizing their information is still being collected and potentially disseminated. While consumers have the right to limit data sharing with unrelated third parties, they are often unaware of those rights, and may have difficulty knowing how to change their preferences.

Congress and federal regulators must act to enhance consumers' privacy. Privacy issues plague a wide variety of financial and nonfinancial services, though they are particularly acute given the sensitive information that may be obtained through access to a financial account.

First and foremost, there must be substantive limits on how companies can use data that cannot be superseded by blanket consent:

- **Companies should not be allowed to use purported consent to permit uses that consumers do not expect or understand.**
- **Use must be limited by purpose.** A consent to use bank account data for credit underwriting should extend to that use alone and should not permit the use of the data for other purposes such as marketing, debt collection, or government licensing.

Consent should also be a product of real choice:

- **Consumers should always have true choice in whether to share their bank account data.** There is too great a risk that creditors will require use of bank account transaction data for all consumers, including those who could have received credit without it. A consumer who already has a "fat file" and a good credit score should be able to rely on that alone without being required to share bank account information. Expansion into bank account information may benefit those consumers who have insufficient credit history information or lower credit scores, but could hurt or risk the privacy of consumers who already qualify for mainstream credit.
- **Consumers should never be required to share bank account transaction data for non-credit purposes,** such as employment, insurance, or government licensing or

benefits. Needs-based government programs should be entitled to only a snapshot of current balances.

- **Consent must be real, knowing and meaningful.** It should never be buried in fine print. It must always be in a separate stand-alone document.

Consumers also need more control over how and when they provide consent or revoke consent:

- **Consent must be limited by data element.** A consumer should be able to choose sharing just cash-flow information (credits, debits, balances) versus sharing cash flow plus the identities of merchants from debit card transactions or the identity of payors who make electronic deposits.
- **Consent should be time-limited and self-expiring.** A consent for credit underwriting should be a single use permission. A consent for account review for an open-end account should expire after one year and require renewal.
- **Consumers should have multiple, simple options for ending data sharing.** Some banks and data aggregators are developing consumer dashboards where they can see who is accessing their data and easily turn it off. Both access points – at the bank and the data aggregator – are necessary. Most consumers do not know who a data aggregator is, and their bank will be the most logical place for them to look. But only the data aggregator may know the multiple other accounts – investment, credit, savings – that may be accessed by an app.

We appreciate that there are industry efforts to achieve more consumer control over data sharing. Again, while voluntary efforts are helpful in the short run, that will not achieve uniform protections or consumer confidence. Ultimately only clear rules of the road with which all actors must comply will fully protect consumers.

Finally, any federal privacy bill must not preempt stronger protections at the state level.

Privacy issues evolve, and no bill will ensure protection into the future. States are more nimble in addressing new problems and can provide the laboratory of democracy for trying new solutions.

D. Consumers need FCRA protections for use of their data

The Fair Credit Reporting Act (FCRA) gives consumers important rights to know what information is being used about them, to ensure that that data is accurate, to require those collecting information to correct errors, and to learn when use of information results in adverse consequences. These rights are important not only for traditional credit reports but also for newer information sources such as the account information accessed through data aggregators.¹⁷

The FCRA was intended to have a very broad scope of coverage. Information is a “consumer report” covered by the FCRA if it is:

- Used or expected to be used or collected in whole or in part to serve as a factor in establishing eligibility for consumer credit or other FCRA-covered purposes (including “a legitimate business need”);
- Pertains to any of seven characteristics, which cover an extremely far-reaching range of information – credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, and mode of living; and
- Issued by a third party that regularly assembles or evaluates such data for money or on a nonprofit cooperative basis.

Thus, almost all third-party data collected for credit decision making purposes should be considered a “consumer report.” Unfortunately, several circuit courts have shown a reluctance to respect the plain language of the FCRA and its broad coverage.¹⁸ **We urge Congress to re-**

¹⁷ The FCRA also limits the dissemination of consumer report information to entities with a “permissible purpose,” fairly broadly defined. 15 U.S.C. § 1681b(a). However, as discussed in Section C above, there should be greater protections and consumer control for financial account data.

¹⁸ See *Kidd v. Thomson Reuters*, 925 F.3d 99 (2d Cir. 2019) (CLEAR product was not a consumer report, despite state agency’s use for employment purposes, because Thomson Reuters had collected information and intended it to be used only for non-FCRA purposes, expressly prohibited its sale or use for FCRA-related purposes, required users to make non-FCRA use certifications, and actively monitored compliance; entity must have a specific intent to furnish a “consumer report.”); *Zabriskie v. Fed. Nat’l Mortg. Ass’n*, 940 F.3d 1022 (9th Cir. 2019) (in a 2-1 decision, holding that Fannie Mae’s Desktop Underwriter program is not a CRA because Fannie Mae did not act with the purpose of furnishing consumer reports to third parties but instead to facilitate a transaction between the lender and itself; relying on *Kidd v. Thomson Reuters* to require specific intent to furnish a consumer report); *Fuges v. Southwest Title*, 707 F.3d 241 (3d Cir. 2012) (objectively reasonable for company that prepared reports on current owners of properties to interpret the reports as outside the FCRA because they allegedly pertained to the property and not to the consumer -- despite the fact the reports included information on judgments personally against the consumer).

affirm the broad scope of the FCRA and that it applies to any-third party data used for credit evaluation purposes.

FCRA protections are critical to protecting consumers when data is used to evaluate them for credit. One of the key issues with alternative data is the level of accuracy of the data. Although one might assume that information drawn from consumers' bank accounts will be accurate, that might not always be the case as errors might arise as the data is passed along, especially with screen scraping, or inaccurate conclusions might be drawn from that data. The FCRA requires accuracy, in that Section 607(b) of the FCRA, 15 U.S.C. § 1681e(b), requires consumer reporting agencies (CRAs) to follow "reasonable procedures to ensure maximum possible accuracy." Section 611(a) of the FCRA, 15 U.S.C. § 1681i(a), gives consumers the right to dispute any errors regarding information about them in a CRA's files.

The FCRA also has specific notice requirements, which are intended to ensure transparency when information about consumers is used. Mostly importantly, Section 615(a) and (h) of the Act, 15 U.S.C. § 1681m(a) and (h), require users to provide adverse action and risk-based pricing notices when information has been used to deny credit or charge a higher price. This ensures that consumers are aware of the sources and types of information that are used against them in credit (and other) decisions, so that they are not left in the dark as to the reasons for decisions that may have critical consequences for their lives.

Furthermore, even if third party information is somehow not considered a consumer report, the FCRA includes a little-known provision that requires transparency in its usage. Section 615(b), 15 U.S.C. § 1681m(b), requires that lenders provide a specific notice if information that fits any of the seven characteristics listed in the definition of "consumer report" is obtained from a person other than a consumer reporting agency and is used to deny credit or charge more for it. This notice must inform the consumer of the right to make a written request for the reasons for the adverse action. Upon such a request, the user must disclose the nature of such information. Section 615(b) should apply to alternative data used for credit decision making even if it somehow escapes the definition of a consumer report.

While banks that use information in a consumer's account at that bank are not covered by the FCRA, data that is not the product of direct experience between the lender and the consumer should be regulated by the FCRA. Compliance with the FCRA is critical for the purposes of accuracy, predictiveness, transparency, and appropriate use.

E. Account data is covered by the ECOA and can result in disparate impacts.

It is critical that the data accessed by data aggregators, like other data, not be used in a fashion that results in discrimination or disparate impacts on consumers in vulnerable communities. Account data will almost certainly exhibit disparities by race because one of the factors used by scoring models is likely to be overdrafts. African Americans are disproportionately affected by bank overdraft practices.¹⁹ And beyond balances and the mere inflow and outflow of funds, bank and credit accounts have a host of sensitive information.

Bank and credit accounts can identify what neighborhood the consumer shops in. Location or geographic neighborhood is one way that creditors have inappropriately assessed creditworthiness by association.²⁰ Given the degree of residential housing segregation that exists in the U.S., location can function as a proxy for race and income and its use by creditors would reflect racial and socio-economic disparities.

Account data can also identify what types of stores, websites or services a consumer uses, or what causes she supports – all of which may correlate with race or other protected classes.²¹ It is

¹⁹ See Pew Charitable Trusts, *Heavy Overdrafters*, April 2016, at <http://www.pewtrusts.org/~media/assets/2016/04/heavyoverdrafters.pdf?la=en> (African-Americans are 12 percent of the US population, but account for 19 percent of the heavy overdrafters).

²⁰ Jeffrey S. Morrison & Andy Feltoich, *Leveraging Aggregated Credit Data and in Portfolio Forecasting and Collection Scoring*, *The RMA Journal*, Oct. 2010, at 47, available at www.forecastingsolutions.com/publications/RMA_OCT2010.pdf (article written by Transunion researchers stating "...aggregated credit data is...helpful to [debt] collectors because it can identify local credit conditions clustered around common demographics. This is especially true for consumers with little or no credit history. For example, if the consumer is living in a ZIP code where the mortgage delinquency rates are climbing or always high, the chance for collection may be significantly less than for those in ZIP codes where the delinquency rate is relatively low and stable.").

²¹ The use of behavioral data has shown indications of racial bias, despite relying on seemingly racially neutral algorithms. In 2013, Latanya Sweeney, a professor of government at Harvard University, led a research project that concluded that Google searches of names more likely associated with black people often yielded advertisements for a criminal records search in that person's name. Hiawatha Bray, *Racial bias alleged in Google's ad results*, *Boston*

even conceivable that account data could reveal who a consumer's friends are and who she exchanges funds with.²²

Thus, use of accounts data could lead to racial or other disparities not based on the individual's credit risk.²³ This is especially true when data that correlates with race or other protected classes is fed into opaque algorithms and machine learning. There is an assumption that algorithms are automatically unbiased or judgment free, but recent research indicates otherwise.²⁴ Recent studies and news reports have shown that computers can discriminate too, from digital mortgages²⁵ to Apple credit cards.²⁶

Actively looking out for and preventing inappropriate disparate impacts is essential. Only by looking for broad patterns can we ensure that we are not perpetuating discrimination and inequality through digital redlining.²⁷

Globe (February 6, 2013) <https://www.bostonglobe.com/business/2013/02/06/harvard-professor-spots-web-search-bias/PtOgSh1ivTZMfyEGj00X4I/story.html>.

²² While the information accessed through data aggregators will not directly include social media information, it is possible that data aggregators could identify social circles through the information in payment accounts like Venmo. Cf. Katie Lobosco, Facebook friends could change your credit score, CNN.com (August 27, 2013) available at <http://money.cnn.com/2013/08/26/technology/social/facebook-credit-score/index.html>. See also Matt Vasilogambros, "Will Your Facebook Friends Make You a Credit Risk?" The Atlantic (August 7, 2015), <https://www.theatlantic.com/politics/archive/2015/08/will-your-facebook-friends-make-you-a-credit-risk/432504/>.

²³ See Carol Evans, Federal Reserve Board - Division of Consumer and Community Affairs, *Keeping Fintech Fair: Thinking about Fair Lending and UDAP Risks*, Consumer Compliance Outlook - Second Issue 2017 (2017), <https://consumercomplianceoutlook.org/2017/second-issue/keeping-fintech-fair-thinking-about-fair-lending-and-udap-risks/> ("[F]intech may raise the same types of fair lending risks present in traditional banking, including underwriting discrimination, pricing discrimination, redlining, and steering. Although some fintech trends may decrease certain fair lending risks, other trends could amplify old problems or create new risks.") [hereinafter "Evans, *Keeping FinTech Fair*"]

²⁴ See Evans, *Keeping FinTech Fair* ("while statistical models have the potential to increase consistency in decision-making and to ensure that results are empirically sound, depending on the data analyzed and underlying assumptions, models also may reflect and perpetuate existing social inequalities. Thus, big data should not be viewed as monolithically good or bad, and the fact that an algorithm is data driven does not ensure that it is fair or objective.").

²⁵ See Robert P. Bartlett, et al., Consumer Lending Discrimination in the FinTech Era, UC Berkeley Public Law Research Paper, December 7, 2017, <https://faculty.haas.berkeley.edu/morse/research/papers/discrim.pdf> (finding that fintech lenders discriminate, albeit 40% less than face-to-face lenders).

²⁶ See Will Knight, Wired, The Apple Card Didn't 'See' Gender—and That's the Problem: The way its algorithm determines credit lines makes the risk of bias more acute (Nov. 19, 2019), <https://www.wired.com/story/the-apple-card-didnt-see-genderand-thats-the-problem/>.

²⁷ See Comments of civil rights, consumer, and other advocacy organizations on Request for Information Regarding the CFPB's Inherited Regulations and Inherited Rulemaking Authorities, Docket No. CFPB-2018-0012 regarding Regulation B and the Equal Credit Opportunity Act (June 25, 2018), <https://www.nclc.org/images/pdf/rulemaking/cfpb-inherited-regs-disparate-impact.pdf>.

As one fintech, Lending Club, put it, disparate impact is an innovation friendly approach:

[T]he disparate impact regime ...

- (a) can address a widely held policy concern [that credit decisioning technology may discriminate without people intending or realizing it] while flexibly accommodating innovation in data, machine learning, and artificial intelligence (AI),
- (b) has not been onerous to comply with in our experience, and
- (c) provides the regulatory stability that supports innovation and investment.²⁸

Data that is used for credit purposes – including data obtained through data aggregators – is subject to the Equal Credit Opportunity Act (ECOA). Data that is using in housing decisions – as bank account cash-flow data theoretically could be – is subject to the Fair Housing Act (FHA). Data that results in disparate impacts in other areas may be subject to other federal or state anti-discrimination laws. **Congress should ensure that the use of consumers’ data does not result in discriminatory impacts against consumers in any context.**

Like the FCRA, the ECOA is a statute with a broad scope. It prohibits discrimination “with respect to any aspect of a credit transaction” on the basis of, *inter alia*, race, color, religion, national origin, sex or marital status, or age. 15 U.S.C. § 1691(a). “Credit” is broadly defined, as is the concept of “creditor,” which is not limited to banks or traditional lenders. 15 U.S.C. § 1691a(d) and (e). Finally, the ECOA is not limited to consumer credit but applies to certain types of business credit as well.

Most importantly for our purposes, Regulation B, which implements the ECOA, expressly notes that “legislative history of the Act indicates that the Congress intended an ‘effects test’ concept ... be applicable to a creditor’s determination of creditworthiness.” 12 C.F.R. § 1002.6(a). The

²⁸ See Comments of Lending Club to Consumer Financial Protection Bureau re: Request for Information Regarding the Bureau’s Inherited Regulations and Inherited Rulemaking Authorities; Maintain Disparate Impact Policy (June 23, 2018), <https://www.regulations.gov/document?D=CFPB-2018-0012-0075>; Comments of the National Consumer Law Center, et al. to the U.S. Department of Housing and Urban Development on HUD’s Implementation of the Fair Housing Act’s Disparate Impact Standard, Docket No. FR-6111-P (August 19, 2019), https://www.nclc.org/images/pdf/special_projects/racial_justice/comments-to-hud-disparate-impact-standard-oct2019.pdf.

effects test is another name for the disparate impact test, and the Official Staff Interpretations explain that the test:

may prohibit a creditor practice that is discriminatory in effect because it has a disproportionately negative impact on a prohibited basis, even though the creditor has no intent to discriminate and the practice appears neutral on its face, unless the creditor practice meets a legitimate business need that cannot reasonably be achieved as well by means that are less disparate in their impact.

Official Interpretations of Reg. B, 12 C.F.R. pt. 1002, supp. I, § 1002.6(a)-2. This effects test essentially has a three-step analysis that consists of:

1. Does the practice have a disproportionately negative impact on a protected class even if it appears neutral on its face?
2. If so, does the practice meet a legitimate business need?
3. Can the same need be reasonably achieved using a less discriminatory alternative?

Like the FCRA, the ECOA also has specific notice requirements. It requires creditors to notify consumers of the action on an application. 15 U.S.C. § 1691(d)(1). If the creditor takes an adverse action, it must provide either a statement of reasons for the action or written notification of the right to such a statement. 15 U.S.C. § 1691(d)(2). This notice must be specific, and must meet the requirements of Regulation B and its corresponding Official Staff Interpretations.²⁹

The notices required by the FCRA and ECOA raise one of the key issues with regards to the use of account data and other forms of alternative data, especially if they are used in artificial intelligence or machine learning – transparency.

²⁹ Reg. B, 12 C.F.R. § 1002.9(b)(2); Official Interpretations of Reg. B, 12 C.F.R. pt. 1002, supp. I, § 1002.9(b)(2). See generally National Consumer Law Center, Credit Discrimination § 10.5.4.2 (6th ed. 2013), *updated at* www.nclc.org/library.

Consumers are entitled to know not only *what* information is being used to assess them, but *how* that information is being used. The use of data aggregators must not reinforce and entrench existing inequality.³⁰

F. The CFPB Should Supervise Data Aggregators

Data aggregators are playing a growing role in consumers' lives. While the industry is still in its relative infancy, data aggregators can impact consumers in many of the same ways that credit reporting agencies can.

As discussed above, there are a number of areas where data aggregators need more oversight, including data security, privacy, and compliance with credit reporting and fair lending laws. Yet to our knowledge, no one – not even likely states – is examining data aggregators.

That should change. The Consumer Financial Protection Bureau has authority over data aggregators as a provider of account information,³¹ as a material service provider,³² and as a provider of a product or service that will likely have a material impact on consumers.³³ The CFPB should define the larger participants³⁴ in the data aggregator market and should supervise them for compliance with all applicable laws within the CFPB's jurisdiction. In addition, as discussed above, the CFPB should already be examining data aggregators that are within the FCRA's definition of "consumer reporting agency" to the extent they are larger participants in the credit reporting market.

We also support proposed legislation to expand the data aggregators that are subject to the Graham Leach Bliley Act's safeguard rules³⁵ and to give the CFPB authority to establish standards under the Act and to enforce data aggregators' compliance. The FTC does not have a

³⁰ A list of studies is available in Chi Chi Wu, NCLC Past Imperfect: How Credit Scores and Other Analytics "Bake In" and Perpetuate Past Discrimination (May 2016), https://www.nclc.org/images/pdf/credit_discrimination/Past_Imperfect050616.pdf.

³¹ 12 U.S.C. § 5481(15)(A)(ix).

³² 12 U.S.C. § 5481(26).

³³ 12 U.S.C. § 5481(15)(A)(x).

³⁴ 12 U.S.C. § 5514(a)(1)(B), (a)(2).

³⁵ 15 U.S.C. § 6801(b).

supervision regime, and there is no reason that data aggregators should not be subject to GLBA supervision the way banks and credit unions are.

* * * * *

The myriad new uses of consumers' account data through data aggregators are intriguing and many will benefit consumers. But we must not allow ourselves to be led down the primrose path of opening up wider and wider access to our personal data without keeping our eyes wide open to where it might lead.

Thank you again for the opportunity to provide my views to the Task Force today. I look forward to your questions.

Lauren Saunders
Associate Director
National Consumer Law Center
On behalf its low income clients

November 21, 2019

Statement for the Record

On behalf of the

American Bankers Association

before the

Task Force on Financial Technology

Of the

House Financial Services Committee

November 21, 2019



November 21, 2019

Statement for the Record*On behalf of the***American Bankers Association***before the***Task Force on Financial Technology****House Financial Services Committee****November 21, 2019**

The American Bankers Association¹ (ABA) appreciates the opportunity to submit a statement for the record for the hearing titled "Banking on Your Data: the Role of Big Data in Financial Services." We believe that responsible innovation in financial services will continue to benefit customers as it has throughout the history of banking. The use of data plays a critical role that can help promote financial inclusion, make it possible to extend credit to many more borrowers, and give customers improved transparency into the financial products they use every day. While ABA has articulated our position on issues such as data privacy² and the use of alternative data³, it is critical to also address how to ensure consumers remain protected when they choose to share their financial data with third parties.

Technology has facilitated the creation of a tremendous amount of consumer financial data. The unprecedented proliferation and availability of this data has enabled the development of new financial innovations that stand to benefit customers. However, the inherent sensitivity of this data and the discussion around the appropriate role of large technology companies in banking highlights the timeliness of this hearing and the need to ensure that financial data are handled appropriately.

As banks innovate, they do so within an established regulatory framework, backed by strong supervision and oversight, that ensures robust customer protection. Innovation is also taking place outside of the banking space. Technology-focused startups are building products that rely on access to consumer financial data. As a result, the demand for consumer financial data has increased dramatically, creating a market for these data.

¹ The ABA is the voice of the nation's \$17.9 trillion banking industry, which is comprised of small, midsized, regional and large financial institutions. Together, these institutions employ more than 2 million people, safeguard \$14 trillion in deposits and extend more than \$10 trillion in loans.

² <https://www.aba.com/-/media/archives/testimonies/energy-commerce-data-privacy-022619.pdf?rev=090cda83dce846378bd6aff86417b587>

³ <https://www.aba.com/-/media/documents/comment-letter/5-17-17abacommentletteralternativedataandmodelingtechniques.pdf?rev=ca13fe8c59304e80abafad4d8c621680>

We believe that if handled appropriately, access to these data can benefit consumers. This is why ABA fully supports the customer's ability to access and share their financial data in a secure, transparent manner that gives them control. Banks and technology companies are collaborating to build the tools that facilitate access to financial data in a way that protects and empowers consumers.

However, it is important to note that sharing financial information is not the same as sharing information about where a consumer ate dinner. Consumer financial data are extremely sensitive and must be protected appropriately. Accordingly, Congress has recognized the sensitivity of financial information and has provided protections for it in the Gramm-Leach Bliley Act of 1999 (GLBA)—obligations that apply to all parties that hold it throughout its lifecycle.

Banks take very seriously their responsibilities to their customers to maintain the highest level of privacy, security, and control over their financial assets and transactions. Today, consumers trust that their financial data are being protected and handled appropriately. This trust is critical to the functioning of the financial system and is the reason banks dedicate significant resources to safeguarding financial data.

Current practices in the data aggregation market, however, may leave consumers exposed and create risks that undermine this trust. Legacy processes known as “screen scraping” require users to forfeit their bank username and password, granting technology companies unfettered access to a customer's most sensitive data. When this happens, customers – often unknowingly – trade their privacy for technology-driven convenience in a way that exposes them to serious financial risk. Consumers often do not fully understand what data is being taken, where it is being sent, or how it is being used.

Banks, aggregators, and technology companies are all aligned on the need to move away from these legacy technologies that create risk to more secure technologies like APIs and are working together to make rapid progress toward this goal.

In 2017, the Consumer Financial Protection Bureau (CFPB) released a set of principles⁴ to support responsible sharing of consumer data. According to then Director of the CFPB, Richard Cordray, “these principles express our vision for realizing an innovative market that gives consumers protection and value.” These principles have served as a flexible bedrock for industry discussion that has facilitated real progress. Since the principles were released, industry collaboration has led to the development of technical standards, model contracts, and other technologies that can help facilitate responsible sharing. We believe that continued industry collaboration is the best way to advance this goal, however there are several regulatory clarifications and other recommendations that would help facilitate responsible data sharing.

ABA Principles for Responsible Data Sharing

ABA has developed a set of principles – consistent with the CFPB and the rest of industry – that we believe ensure that consumers remain protected when they share their financial data.

1. Access

Banks support our customer's ability to use third-parties to access their financial account data in a way that is safe and secure.

⁴ https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf

2. Security

Consumers deserve bank-level security and protection regardless of where they choose to share their data. This means that consumer data are treated the same – and subject to GLBA protections – whether at a bank or a third party.

3. Transparency

Consumers must have transparency about how companies use their financial data. It should be clear to consumers what data a technology company are accessing, how long the company is holding this data, and how it is using the data.

4. Control

When consumers share their financial data they should have control over what information is shared and how it is used. Intuitive control would allow consumers to see easily who is authorized to receive their data, modify what access they have, and revoke that access when a service is no longer used. If consumers can easily control the data being accessed, they can better understand what is being used and protect themselves accordingly.

5. Minimization

Consumers should expect that data-sharing is limited to the data that are needed to provide the service they have authorized and only maintain these data as long as necessary. Limiting sharing to necessary data helps minimize privacy risks and allows consumers to better understand what kind of data is being accessed and used. Services that go beyond financial account aggregation, such as money movement, present different risks and should be subject to separate agreements and require separate informed consent.

Industry Driven Progress

ABA believes that collaboration between banks, technology companies, and data aggregators is the best way to promote an ecosystem that facilitates responsible data sharing. The significant industry progress in recent years demonstrates this to be true. There are several separate, but related pieces needed to build an ecosystem that supports responsible sharing that include 1) technical standards to securely move the data from point A to point B, 2) contracts that make it easy for banks to work with aggregators, and 3) permissioning systems that track and manage consumer consents.

Technical Standards (APIs):

It is critical that we move away from legacy processes like “screen scraping” that leave consumers exposed to risk and adopt technical standards that can securely move data from banks to aggregators and beyond.

Application Programming Interfaces (APIs) serve as universal adaptors for data, allowing for more secure transmission of data between systems in a standardized format. This empowers customers to share financial data without forfeiting their bank-user credentials. For more information on how APIs work, please refer to ABA’s Understanding APIs report⁵.

This is an area where industry has made significant progress. In the fall of 2018 banks, aggregators, and technology companies came together to found the Financial Data Exchange (FDX) out of a recognition that progress was only possible with the participation of a diverse group of stakeholders. FDX is a nonprofit formed to develop a common, interoperable, royalty-free standard for secure and convenient consumer

⁵ <https://www.aba.com/-/media/documents/reference-and-guides/understanding-apis.pdf>

and business access to their financial data. FDX has developed an API that can facilitate secure data sharing among all of these parties. ABA is a member of FDX alongside many of our banks, technology companies and aggregators.

The nature of innovation means that things are constantly changing, and it is important to note that no one technology will always be the right tool to facilitate secure data transmission. There are also many different APIs for different solutions and while APIs are the best technology today, we need the flexibility to adopt new technologies as the business of banking evolves. Technology mandates would lock us into legacy technologies and risk undermining both safety and innovation.

Legal Contracts

In order to move to API standards, banks and data aggregators must enter into legal contracts that dictate how data is accessed and protected. These contracts are critical to ensuring that customers remain protected and that their data is afforded bank-level protections when it is shared.

With legacy practices like “screen scraping” the bank has no direct relationship with an aggregator. This is because from a bank’s perspective, the aggregator looks like their customer. They effectively show up on a bank’s website and enter login credentials and access an account.

Implementing an API requires a contract that governs the use of that API and ensures the bank’s data security and privacy requirements are being honored. However, negotiating these contracts is an expensive and time-consuming process, often taking as long as 12 months. While larger institutions have the resources and scale to engage in these negotiations, community banks typically lack the resources to negotiate directly with aggregators.

The Clearing House (TCH) recently released a template agreement known as the Model Data Access Agreement designed to improve the process of contract negotiations. The model agreement was designed in consultation with banks and technology companies. This model contract is voluntary and is intended to be modified as individual circumstances may warrant. Additionally, it avoids taking positions on commercial terms that would be negotiated between parties. The contract does, however, provide for a common ground from which banks can engage with aggregators.⁶

While significant progress is being made, concerns remain about some aspects of contracts, including the timing, retention, and deletion of existing data.

Permissions

The third key component of empowering consumers to securely share their financial data is a permissioning system. Unlike the first two efforts, these are not industry-wide efforts, but typically done at the bank level as it is part of a bank’s digital experience. These systems are key to facilitating transparency and consumer control over their data. Permissioning systems track where a consumer has consented to share their financial data and provide a transparent portal to that allows them understand what data are shared, limit the data that are shared, and revoke access altogether.

We have seen many large banks unveil permissioning platforms, Wells Fargo’s “Control Tower” is just one example. However, this technology is largely unavailable to community banks today as it is not offered by

⁶ <https://www.theclearinghouse.org/connected-banking/model-agreement>

their core banking platforms. These core providers play a critical role in ensuring that community banks have the tools to meet market demand and remain competitive in a digital economy.

ABA Recommendations

While we believe a market-driven approach is the best way to empower consumers to control their financial data, there are several regulatory and legal clarifications that can help give certainty to the market that will allow the private sector to more quickly make progress.

We believe the following recommendations are necessary to ensure that customers of all banks – regardless of their asset size – can control their financial data and fully benefit from financial innovation.

Core providers should offer community banks the tools to facilitate secure data sharing. Community banks rely on technology infrastructure from companies that provide software systems known as core banking platforms. Core technology supports everything from accepting deposits to originating loans, all of which tie into operating the core ledger that keeps track of customers' accounts. For many banks, their core provider is the heart of their IT infrastructure. Without the support of these core providers, it would be impossible for community banks to offer the API access or permissioning systems that the market demands today.

ABA has engaged with the core providers through its banker driven Core Platforms Committee, made up of community and mid-sized banks, in an effort to strengthen relationships between banks and cores. One of the key priorities that this committee has identified is data access. Community banks often struggle to quickly and easily access the data held in their core platforms, much less facilitate access for third parties. For community banks to remain competitive, it is critical that the core providers engage in industry efforts and adopt technologies that facilitate the secure data sharing that customers demand.

The CFPB should clarify that GLBA applies to data aggregators

U.S. law has long accorded special status to consumer financial information given the sensitivity of the information. To ensure consumer financial information is properly secured, it is subject to laws related to privacy, data protection, and restrictions on data use and accessibility. For example, the Gramm-Leach-Bliley Act of 1999 (GLBA) imposes on financial institutions obligations to respect customer privacy and to safeguard financial information. Specifically, Section 501 of that law imposes on financial institutions an "affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."⁷

Consumers should expect that their financial data is protected whether it is held by a bank or a data aggregator. As discussed above, GLBA provides a robust framework to protect "nonpublic personal information" of a consumer that is held by a "financial institution." ABA believes that data aggregators fall under the GLBA's definition of "financial institution" and therefore should be subject to all the rules that apply to all other financial institutions. This assures that data protections apply consistently regardless of where the data originated, where it is transferred, and the type of company is using or storing the data.

Congress used an intentionally robust and expansive definition of "financial institution" in GLBA, which encompasses "any institution the business of which is engaging in financial activities as described in [the

⁷ 15 U.S.C. § 6801(a)

November 21, 2019

Bank Holding Company Act of 1956, section 4(k).⁸ This definition includes not only banks, but as interpreted by the Board of Governors of the Federal Reserve, the definition encompasses any entity that provides data processing, data storage and data transmission services for financial data. In other words, GLBA clearly applies to data aggregators.

While we believe it is clear that GLBA applies to data aggregators, any confusion in the market could stifle the progress toward moving to more secure methods of data sharing. Therefore, we believe that Congress should encourage the CFPB to articulate clearly that data aggregators fall within GLBA's definition of "financial institution" subject to the requirements of GLBA as they apply to other financial institutions. This would ensure that consumers receive the GLBA security protections as implemented by the Bureau's Regulation P and the FTC's Safeguards Rule.

The CFPB should bring data aggregators under direct supervision

By the nature of their business, data aggregators hold a tremendous amount of consumer financial data. It is estimated that data aggregators hold the consumer login credentials for tens of millions of customers. Despite this, many consumers don't know that these intermediaries exist or how much of their information is being collected. In most cases consumers do not have a direct relationship with these companies and must trust that their data is being handled appropriately.

As discussed in above, ABA believes that data aggregators are subject to GLBA, but their compliance with its privacy and security obligations is not clear and, more important, is not subject to supervision or regular examination. Proactive supervision is critical to identifying risks before any harm is done to consumers.

A cornerstone of Title X of the Dodd-Frank Act was the authority given to the CFPB to establish a supervisory program for nonbanks to ensure that federal consumer financial law is "enforced consistently, without regard to the status of a person as a depository institution, in order to promote fair competition." Experience demonstrates that consumer protection laws and regulations must be enforced in a fair and comparable way if there is to be any hope that the legal and regulatory obligations are observed. ABA believes that establishing accountability across all providers of comparable financial products and services is a fundamental mission of the Bureau. This is especially important for data aggregators, given the sensitive consumer financial information they store and process.

The bulk of the data processing in this area is managed by a select group of large companies. Accordingly, Congress should urge the CFPB to initiate expeditiously the rulemaking process under Dodd-Frank Act 1024 to define those "larger participants" in the market for consumer financial data that will be subject to regular reporting to and examination by the CFPB. Once the Bureau has imposed supervisory authority over the larger data aggregators, the CFPB can better monitor – and react to – risks to consumers in this rapidly evolving marketplace.

The CFPB should clarify liability for unauthorized transactions under Regulation E

Under §1005.14 of Regulation E, a person that provides an electronic fund transfer service to a consumer is generally subject to Regulation E, with certain modifications, if it (1) issues an access device that the consumer can use to access the consumer's account held by a financial institution and (2) has no agreement with the account-holding institution regarding such access.

⁸ 15 U.S.C. § 6809(3).

Data aggregators that permit consumers to initiate electronic fund transfers from accounts held at financial institutions that do not have an agreement with the financial institution are “service providers” under Regulation E, as they issue “access devices”⁹ that may be used to permit electronic fund transfers to and from the account. As service providers, they are liable for unauthorized transactions under Regulation E as well as certain other provisions.

Imposing liability for unauthorized transactions under these circumstances is appropriate and fair. The data aggregator is in the best position to control the risk of unauthorized transactions conducted through its system. In contrast, the financial institution holding the account has no relationship with the data aggregator, no knowledge of, and no power over the data aggregator’s security system. This approach is consistent with payment system laws which generally assign liability to the party that is in the best position to avoid a loss and manage the risk of a loss. Indeed, it is for these reasons that Regulation E assigns liability to service providers.

Moreover, other provisions related to service provider responsibilities support classifying data aggregators as service providers under Regulation E. These include requirements related to error resolution, disclosures, the prohibition against the issuance of unsolicited access devices, and change in terms notices.

ABA believes that data aggregators providing electronic fund transfer services are service providers under Regulation E. To avoid any ambiguity, Congress should urge the Bureau to confirm this in the regulation or official commentary.

Banking regulators should clarify that bank agreements with data aggregators do not constitute third-party vendor relationships.

Notably, data aggregators are authorized by and act on behalf of bank customers, not the bank. When banks enter into agreements with data aggregators, they do so to reduce risk and to apply additional protections to their consumers’ data as it leaves the secure banking environment.

Section 7 of the Bank Service Company Act (BSCA) requires banks to notify their regulators of contracts or relationships with certain third-party service providers and undertake due diligence on these partners. This is intended to capture relationships where banks partner with third parties to deliver experiences to their customer. In the case of data aggregators, there is no such partnership. A consumer has directed his or her bank to share their data; a bank’s contract simply lays out the terms for how that data is shared and provides a more secure portal for doing so. Such a contract should not result in the data aggregator becoming a third-party service provider to the bank. Rather, the relationship should be regarded as a customer-aggregator relationship.

A lack of clarity about the applicability of the BSCA to contracts with data aggregators could stifle adoption of more secure technologies that provide additional protections for customers. Moreover, banks have little ability to perform due diligence or supervise these data aggregators because the aggregators have no

⁹ Under Section 1005.2(a) of Regulation E, “Access device means a card, code, or other means of access to a consumer’s account, or any combination thereof, that may be used by the consumer to initiate electronic fund transfers.”

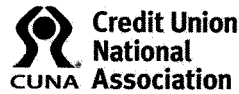
November 21, 2019

incentive to respond to bank due diligence requests since there is no business relationship between the bank and the aggregator.

Conclusion

Today, technology is fundamentally changing the way financial services are being delivered. Consumer financial data is more available and widely shared than ever before. ABA believes that innovations in financial services present tremendous value. This value is only realized when innovations are delivered in a responsible manner that maintains the trust that is critical to the functioning of our financial system. The focus on the consumer financial data market is important.

By fairly addressing both the opportunities and risks, we have the ability to give consumers innovative services that they can trust. Customers need security, transparency and control to unlock the true potential of fintech and take charge of their financial future.



Jim Nussle
President & CEO

Phone: 202-508-6745
jnussle@cuna.coop

99 M Street SE
Suite 300
Washington, DC 20003-3799

November 21, 2019

The Honorable Stephen F. Lynch
Chairman
Task Force on Financial Technology
U.S. House of Representatives
Washington, DC 20515

The Honorable Tom Emmer
Ranking Member
Task Force on Financial Technology
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Lynch and Ranking Member Emmer:

On behalf of America's credit unions, I am writing to express our views ahead of the hearing titled "Banking on Your Data: The Role of Big Data in Financial Services." The Credit Union National Association (CUNA) represents America's credit unions and their 115 million members. Thank you for holding this important hearing and including our views in the hearing record.

We appreciate the Task Force holding this important hearing to explore the role of big data in financial services and for producing discussion drafts of bills that would enhance the protection of consumers' financial data when possessed by any entity or business. Credit unions are deeply concerned that Americans' financial wellness is compromised by inconsistent privacy and security standards applied to businesses that possess, process or transport consumers' nonpublic personal information (NPI). We fear that non-depository institutions, such as data aggregators and other businesses that collect and sell data put Americans' financial well-being at risk by not protecting the data and by using it in ways that target marginalized communities. Furthermore, misuse of NPI makes it more difficult for credit unions to deliver necessary financial services to these communities.

As you know, credit unions and banks are subject to requirements of the Gramm-Leach-Bliley Act (GLBA), which imposes data protection requirements and regulates how credit unions and banks can use their members' and customers' NPI. Credit unions and banks cannot share nonpublic NPI to nonaffiliated third parties unless they provide a notice and members/customers can opt-out. Credit unions and banks must also provide annual privacy notices and disclose what NPI is shared with third parties. The consumer protections in GLBA help to ensure that NPI held at credit unions and banks is protected from theft and misuse and that consumers are well informed of how it is used for necessary business purposes.

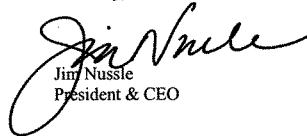
Applying GLBA's protections to any business or entity that possess NPI is a good first step that will enhance protection for Americans' financial information. Although CUNA supports this approach, we would prefer that Congress move beyond GLBA and develop a uniform privacy and data security law that regulates data and privacy protections based on the type of data instead of the current sector-specific approach. While the sector-specific approach worked well when American's health and financial information were mainly in the possession of health care providers and depository institutions, Big Data's insatiable appetite for NPI has made regulation under the current framework difficult at best.

Although credit union members are protected by GLBA's requirements for the NPI they collect and maintain possessed by credit unions, the time has come to abandon GLBA for new laws that protect NPI no matter who possesses, transports or processes the information. CUNA supports legislation that would:

- Apply data privacy and data security standards to everyone — all business, institutions and organizations — and hold each link in the transaction journey accountable;
- Create equal expectations and protections by harmonizing inconsistencies through new legislation that protects sensitive information based on the type of information rather than the type of entity that possess it;
- Create a national standard that is the ceiling for requirements;
- Base protections on strong standards that protect data; and
- Safeguard consumer protections by providing mechanisms to address the harms that result from privacy violations and security violations, including data breaches.

We look forward to working with the Task Force on ways that new legislation can protect Americans' personal information. Thank you for your consideration of our views.

Sincerely,



Jim Nussle
President & CEO



1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electran.org

November 21, 2019

The Honorable Stephen Lynch
Chairman, Task Force on Financial Technology
Committee on Financial Services
United States House of Representatives
Washington, DC 20515

The Honorable Tom Emmer
Ranking Member, Task Force on Financial Technology
Committee on Financial Services
United States House of Representatives
Washington, DC 20515

Dear Representatives Lynch and Emmer:

On behalf of the members of the Electronic Transactions Association (ETA), I am pleased to submit this statement for the record on the important topic the Task Force on Financial Technology is undertaking on Big Data in Financial Services.

ETA is the leading trade association for the payments industry, representing over 500 companies that offer electronic transaction processing products and services; its membership spans the breadth of the payments industry to include independent sales organizations, payments networks, financial institutions, transaction processors, mobile payments products and services, payments technologies, equipment suppliers, and online small business lenders.

ETA member companies include traditional financial institutions and financial technology (FinTech) companies. ETA members are dedicated to continuously driving innovation in the payment space and values the importance of a financial ecosystem that provides consumers and small businesses with financial products and services that are convenient, secure, and reliable.

As part of this innovation, access to financial data and information is an important aspect. Access to data involves consumers, traditional financial institutions, as well as FinTech companies and other financial service providers, including data aggregators and third-party application providers. The two groups - traditional and FinTech companies - are working together to share data to serve consumers and small businesses.

In the context of data aggregation, the convergence between the traditional and FinTech companies is driven by the themes of consumer access, choice, and control. ETA member companies use consumer account data to develop new products and services that empower consumers to manage their finances. These products and services include fraud screening and identity verification, personal financial management, and bill payment. Such products and services help consumers and small businesses make smarter spending, savings, and investment decisions and live their lives more efficiently and effectively.

While ETA supports consumers and small businesses having choice and control over how their data is used and shared the many benefits of innovation should not come at the expense of consumer protection. In this regard, the question of increased access and control over financial data and information triggers other important issues such as cyber security, transparency, and disclosure.

ETA and its members believe that the adoption of principle-based, industry-led safe and secure data access methods across the ecosystem and other minimum standards are necessary to address these issues and corresponding risks, including the risk of fraud in the event of a data breach. ETA also supports a performance-based standard that allows for flexibility and innovation, rather than a prescriptive requirement that necessarily favors one method over another.



1620 L Street NW, Suite 1020
Washington, DC 20036

202.828.2635
electran.org

Security performance standards need to be developed to ensure technology is sufficient (and continually reviewed), access is limited, consent-based, and storage of data occurs. However, it is imperative that technology standards do not mandate a specific type of technology, but remain flexible enough to ensure industry leading safeguards, and allow for innovation.

Consumers must have confidence that their data is adequately protected by all applications, systems, and providers that have access to it. This includes use of technology such as application programming interface (APIs) and tokenization; however, ETA cautions the adoption of one technology over another as the aforementioned technologies are not the only secure options available today. More importantly, technology will continue to evolve over time, so standards must not stipulate specific types of technologies, but rather provide that entities follow applicable laws and industry best practices regarding data security. In order to fully achieve security, a shared set of standards is needed that can be applied and updated on an ongoing basis.

As technology and innovation are constantly evolving and continue to shape how information is created, accessed, stored, and disposed of, policy must remain adaptable and should not impose rigid rules that have the effect of unnecessarily restraining innovation or imposing unnecessary costs or burdens on industry. Although the government will undoubtedly play an instrumental role in guiding the dialogue, ETA cautions against mandating a specific requirement in this area as there is no guarantee the method would improve upon existing methods, but there would be a significant risk that any such method would quickly become outdated, all while imposing significant costs on industry to conform their existing practices to a government-regulated approach.

ETA members operating globally have already been involved in the creation of similar frameworks in other jurisdictions, like the UK, and are determined to share their experiences and challenges, and provide their expertise to help securing the best outcome for customers and businesses.

The U.S. is uniquely positioned to benefit from the experience and regulatory proposals being adopted or considered by its international counterparts and to adopt best practices and market-led initiatives that work best within our environment and market structure.

We appreciate your leadership on this important issue and look forward to continuing to work with the Task Force on Financial Technology. If you have any questions, please feel free to contact me directly at stalbott@electran.org.

Sincerely,

A handwritten signature in black ink, appearing to read 'Scott Talbott', is written over a light blue horizontal line.

Scott Talbott
Senior Vice President of Government Affairs
Electronic Transactions Association

**VIA ELECTRONIC SUBMISSION**

November 20, 2019

The Honorable Stephen Lynch
Chairman
Task Force on Financial Technology
House Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC 20515

The Honorable Tom Emmer
Ranking Member
Task Force on Financial Technology
House Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Lynch and Ranking Member Emmer:

The Financial Data and Technology Association of North America (“FDATA North America”) appreciates the opportunity to submit a letter for the record for the House Financial Services Committee’s Task Force on Financial Technology’s hearing entitled “Banking on Your Data: the Role of Big Data in Financial Services.” As the leading trade association advocating for consumer-permissioned, third-party access to financial data, FDATA North America and its members strongly believe that an open banking framework is required to provide for the appropriate balance of innovation, improved consumer and small business financial access and opportunity, and end-user protection. The first, critical step in the creation of such a framework in the United States is the provision of the legal right for consumers and small businesses to their financial data, thereby empowering them to leverage their own data for improved financial outcomes through technology-based tools that can help them improve their financial wellbeing.

FDATA North America was founded in early 2018 by several firms whose technology-based products and services allow consumers to better manage their finances, improve their financial wellbeing, and/or enable small businesses to provide higher-quality products to their customers. We count innovative leaders such as the Alliance for Innovative Regulation, Betterment, Envestmet Yodlee, Flinks, The ID Co, Intuit, Kabbage, Lendified, Mogo, Morningstar, MScience, MX, Petal, Plaid, Qeustrade, Quicken Loans, TransUnion, VoPay, and others, as our members. We are 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, lawmakers, and supervisory bodies internationally contemplating, designing, and implementing open banking frameworks.

Though the title of the hearing the Task Force is holding implies a robust ecosystem in which Americans’ data can be utilized in the financial system, there currently exists no legal right for consumers or small businesses to leverage their own financial data through the financial provider of their choice. This absence limits consumer choice in determining the products and services best suited to their individual financial situations and hinders competition, improved pricing, and innovation. The financial needs of individual consumers, their families, and small businesses vary widely, and lack of access to innovative financial products, and transparency of



those products, limits options that could be life changing, enabling consumers to benefit from services they previously could not qualify for or afford, and, unfortunately, sometimes forcing them to turn to products of a more predatory nature.

Additionally, because consumers have no legal right to access and share their data, the system for sharing data between financial institutions and fintechs is cumbersome and lacks transparency to the end user, who, in a well-managed open banking system, is appropriately at the center of the ecosystem. Financial institutions, fintechs and aggregators all recognize that key policy principles must be developed to make consumer financial data more securely accessible and portable – including standards relating to liability, transparency, and accountability – but, currently, the only tool available to the industry to address these issues is individual bilateral agreements between financial institutions, aggregators, and fintechs. It is impossible for the thousands of financial institutions in the United States to negotiate and execute opaque bilateral agreements with every financial aggregation firm. Moreover, even if this outcome were practical, the individual terms between counterparties would likely differ from financial institution to financial institution and from aggregator to aggregator, leading to an unlevel playing field in which some consumers and small businesses are provided with more financial opportunity than others, merely because of the terms of a bilateral agreement between their bank and an aggregation firm to which the end user was not party. This complex array of agreements further limits transparency for consumers.

To appropriately encourage innovation in the financial sector for the benefit of consumers and small businesses, policy changes and comprehensive oversight are necessary to ensure the full legal right of the consumer to use their financial data safely and securely. A well-structured consumer-directed regime would allow individual consumers and small businesses to choose to provide access to their financial data to providers of their choice; to have agency over who has access to various elements of their financial data, and, importantly, to revoke that access when or if they ever see fit. Additionally, such a regime would necessarily have to provide a level of oversight over third-party technology providers and would have to begin the process of more appropriately accounting for potential liability risk throughout the 21st century financial system.

To achieve these goals, FDATA North America strongly supports legislation sponsored by Consumer Protection and Financial Institutions Subcommittee Chairman, Rep. Gregory Meeks (D-NY). H.R. 4047, the Open Banking Study Act, would take a small but critical step toward ensuring consumers and small businesses have greater control and flexibility with regard to the financial products and services they choose. The legislation would merely require the Federal Reserve, the Consumer Financial Protection Bureau (CFPB), the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA) to report to Congress what actions both they and the entities they regulate have taken to advance open banking in the United States. The Open Banking Study Act does not enact new policies, impose new requirements upon the regulatory agencies, or establish any new standards in the marketplace. Instead, it would begin the process of identifying outdated processes and guidance that will need to be modernized to better harness



innovation in the financial services markets, as well as how best to utilize those authorities Congress has already bestowed on regulatory bodies, including third-party vendor risk management oversight and Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, which provides the CFPB with the ability to ensure financial institutions make available to consumers their own financial data.

Countries around the world are quickly embracing the notion that the consumer should be in control of their financial data, and without recognizing this modernized approach, the United States could fall behind as the world leader in digital innovation and market competition. The open banking policies, rules, and regulations embraced by countries around the world – including the United Kingdom, Australia, Canada, and Singapore, just to name a few – have improved the global competitiveness of these nations and have enhanced financial inclusion for their citizens. FDATA North America respectfully suggests that, at this critical time in the evolution of the financial services industry, Congress initiate a holistic review of those regulations and policies that may require modernization to reflect the changing financial ecosystem and build a future that benefits consumers and small businesses.

The Open Banking Study Act would be a modest but critical first step toward increasing consumer confidence, providing a standardized regulatory and policy regime that supports safety and soundness, and supporting a platform that embraces technological innovation. By not acknowledging the advancements made in other countries that put the consumer first, the United States runs the risk of falling behind globally and supporting an outdated and unsecure financial system.

FDATA North America welcomes this hearing of the Task Force and looks forward to working with you and your colleagues on these important issues in the months ahead.

Sincerely,

Steven Boms
Executive Director
FDATA North America



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

November 21, 2019

Submitted Electronically

The Honorable Stephen F. Lynch
 Chairman
 Task Force on Financial Technology
 U.S. House Financial Services Committee
 2129 Rayburn House Office Building
 Washington, DC 20515

The Honorable Tom Emmer
 Ranking Member
 Task Force on Financial Technology
 U.S. House Financial Services Committee
 2129 Rayburn House Office Building
 Washington, DC 20515

Hearing Titled “Banking on Your Data: The Role of Big Data in Financial Services”

Statement for the Record:

Dear Chairman Lynch and Ranking Member Emmer:

Fidelity Investments (“Fidelity”)¹ commends your bipartisan leadership on the important topic of data and financial services and welcomes the opportunity to share our views. In this statement for the record, we provide concrete ways to make consumer-directed financial data access safer and more transparent for financial institutions, data aggregators, fintech firms, and—most importantly—consumers.

My name is Stuart Rubinstein and I am President of Fidelity Wealth Technologies and Head of Data Aggregation. I am also President of Akoya, which is a new company focused on helping Fidelity and other institutions enable consumers to direct financial firms to provide secure access to account data and documents to third parties. Fidelity is a leading provider of investment management, retirement planning, portfolio guidance, brokerage, benefits platforms, and other financial products and services to more than 30 million individuals, institutions, and financial intermediaries with \$8 trillion in assets under administration. Our goal is to make financial expertise broadly accessible and effective in helping people live the lives they want and save for retirement.

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 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 access practices. Accordingly, we recommend this Task Force and other policymakers provide the marketplace with clear direction on how best to protect consumers’ financial data.

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.

November 21, 2019

Page 2 of 7

Current State of Financial Data Aggregation

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 his or her 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 as a financial services firm we 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, 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 data access technologies by adopting, for example, application programming interfaces (APIs),² the vast majority of financial data aggregation participants use the outdated and risky screen scraping model.

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

² 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.

November 21, 2019

Page 3 of 7

security, and identity theft. Because in most cases consumers go directly to data aggregators or their commercial clients³ and not their financial institution to request access, 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 aggregation practices.⁴ Correspondingly, regulators have appropriately focused heightened concern on the 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.⁵ 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.⁶

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 feedback on its recent request for comment on Financial Technology in the broker-dealer industry.⁷

³ 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.

⁴ 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>.

⁵ 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.

⁶ 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>.

⁷ 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.

November 21, 2019

Page 4 of 7

In late 2018, 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.⁸ 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 access to 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's Subcommittee on Consumer Protection and Financial Institutions⁹ and the Senate Banking Committee (SBC)¹⁰ outlining our views on financial data aggregation. We also submitted a response to the SBC's February 13, 2019, request for feedback on data privacy, protection, and collection that is substantially similar to the arguments made in this statement for the record.¹¹

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 access 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 to encourage policymakers and the private sector to evaluate safer consumer-driven financial data access technologies. We presented these five principles to the Committee in September 2018, but reiterate them here:

1. **We strongly support consumers' right to access their financial account data and provide access to 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

⁸ U.S. DEPARTMENT OF THE TREASURY, A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES: NONBANK FINANCIALS, FINTECH, AND INNOVATION (July 31, 2018), *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.

⁹ 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>

¹⁰ See *Fintech: Examining Digitization, Data, and Technology: Hearing Before the S. Banking Comm.*, 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>.

¹¹ Letter from Stuart Rubinstein, President, Fidelity Wealth Technologies and Head of Data Aggregation, to the Senate Banking Committee (March 15, 2019), *available at* https://www.banking.senate.gov/imo/media/doc/Data%20Submission_Fidelity%20Investments1.pdf.

November 21, 2019

Page 5 of 7

is broad enough to encompass security, transparency, and cybersecurity protections for consumers.

2. **Data access must be safe, secure, and transparent.** We firmly believe credential sharing makes the system less safe for consumers, aggregators, and financial institutions alike. While we strongly support customers directing access to their financial account data, the security of that data, customer assets, and financial institution systems must be our primary concern.
3. **Consumers should provide affirmative direction and instruction to financial institutions to provide access to their data to third parties.** Rather than require 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 customer credentials is mistaken for authorized access.
4. **Third parties should access only the data needed for the consumer to achieve their goals.** There should be a tight nexus between the service provided and the information accessed 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 access 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 access ecosystem, there are roadblocks preventing wider adoption of safer 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 institutions, aggregators, and fintech firms should be swiftly moving to safer data access technologies. Accordingly, we

November 21, 2019

Page 6 of 7

recommend to this Task Force the following consumer and investor protection focused legislative 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 specified third parties to access their data. Congress should create consumer protection principles governing how financial institutions, aggregators, and fintech firms access consumers' financial account data.
- **Minimum consumer protection standards for data access:** While consumers have a right to access their financial account data and permit access to third parties, that access must be done pursuant to minimum standards of security and transparency. Third parties that wish to access 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 incentivize firms to adopt newer, safer technologies when they become available and scalable.
- **Affirmative direction by consumer:** Consumer-directed access to 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 for a specific purpose:** When consumers direct financial institutions to permit third party access to 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 consumer-driven financial data access 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 or is otherwise responsible for a consumer harm

November 21, 2019

Page 7 of 7

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 access 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 most of these problems. However, we are having difficulty translating considered discussion into actual momentum. Indeed, Fidelity is working hard to facilitate safer consumer-directed financial account data access and aggregation technologies. However, the time has come for Congress to act. We must make consumer-directed access to 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 Task Force with additional information, perspective, or resources as you work through these critically important issues.

Sincerely,

A handwritten signature in black ink, appearing to read "Stuart Rubinstein". The signature is fluid and cursive, with the first name "Stuart" and last name "Rubinstein" clearly distinguishable.

Stuart Rubinstein
Head of Data Aggregation
President, Fidelity Wealth Technologies



**Statement for the Record to the House Committee on Financial Services Task Force on Financial
Technology Hearing: "Banking on Your Data: The Role of Big Data in Financial Services"
November 21, 2019**

Submitted by Finicity

Chairman Lynch, Ranking Member Emmer, and Members of the Task Force; thank you for the opportunity to submit a statement for the record to the House Committee on Financial Services Task Force on Financial Technology's hearing entitled, "Banking on Your Data: The Role of Big Data in Financial Services."

Steve Smith
Co-founder & CEO

434 W. Ascension Way, Suite 200
Salt Lake City, UT 84123
www.Finicity.com

Technology is transforming the financial services industry at the speed of light and “fintech” innovations are offering immense value to consumers and businesses alike. However, these rapid shifts introduce the need for new standards and safeguards that protect all constituents across the financial system, most importantly the consumer.

Industry participants, policymakers, regulators, and other stakeholders must all work together to ensure that innovation and consumer protection are aligned. No one group can determine the way forward alone.

One of the most transformative technology disruptions has been the availability and use of data. Organizations of all sizes are now mining and leveraging their business data to improve efficiency, gain market insight, increase profitability, and enhance customer experiences. In the same way, individuals and families are realizing the value of their own financial data in making wise financial decisions, accessing credit, and enhancing their overall financial health.

Fintech innovation places consumers in control of their own financial universe by providing access to personal financial data and by facilitating the permissioning of that data in a multitude of applications. However, advancing consumer empowerment and unleashing the potential of tapping into one's own data is wholly predicated on one core principle—the right of the consumer to own, employ, and easily access their data. There is much to be done to ensure that this right to data is fully realized.

Finity stands at the intersection of the financial data ecosystem that is empowering consumers with their own data. We provide data access and insights so that individuals and businesses can harness the power of their own financial data to improve their financial health. Finity accomplishes this mission through data connections to financial institutions. These connections enable consumers to permission their data for use in third-party applications or solutions. Consumers can now access their data in personal finance management and budget applications or use it to speed up the process of getting a loan. They can verify and authenticate bank accounts for instant payments and even contribute data for a more accurate credit report and score. Finity allows consumers to leverage their own financial data in a myriad of innovative ways every day.

A Roadmap for Empowerment and Innovation

Finity believes that the market is at a critical juncture in financial services innovation. In order for consumer-centric innovation to continue, industry, policymakers, consumer groups, and other stakeholders must all collaborate to make the right decisions. With this in mind, Finity offers a high-level overview of the current marketplace and a roadmap for moving forward. The roadmap has three facets:

1. **Guiding Core Principles:** The financial data ecosystem must enhance consumer awareness and protection in five critical areas: control, access, transparency, traceability, and security. These issues are paramount to earning consumer trust in the data sharing process. They must be addressed head-on.
2. **Financial Industry Collaboration:** Time and again, industry and self-regulation has proven to be more effective and efficient than government intervention when it comes to industry standardization and best practices. Such industry efforts preserve the pace of innovation and also provide the tools and incentives necessary to

eliminate poor business practices and bad actors from an industry. This enables market participants to focus on the consumers they serve. Finity is a board member of the Financial Data Exchange (FDX) and believes this organization is best suited to provide standards, liability frameworks, collaborative industry certification and vetting services, and best practices for the consumer-permissioned financial data services industry in the areas listed above.

3. Regulatory Clarity and Modernization: The U.S. financial regulatory system is splintered in its authority and jurisdiction over matters concerning consumer-permissioned financial data. For this reason, and as stated above, industry collaboration is likely to lead to the best outcomes for consumers. However, in a few key areas, regulatory and statutory clarity and modernization is needed to ensure consumers have full access to the data they own and that the appropriate safeguards are in place related to privacy and secure data use.

Market Overview

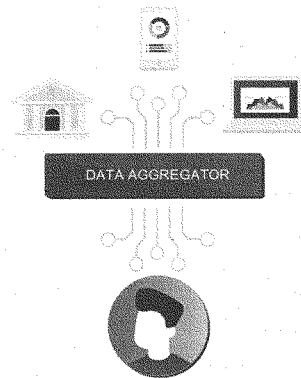
In order to fully contextualize the way consumer-permissioned financial data is transforming financial services, it is important to fully understand both the market participants as they exist today and the concept of consumer-permissioned data.

Market Participants

Participants in the financial data services industry ecosystem work together to create efficient processes and to enable fast innovation. And while roles are often distinct, as the ecosystem develops many of these roles are being fulfilled by the same organization. Therefore, it is important to develop standards and policies that are tied to use cases rather than organizations.

Key market participants include:

- Consumers: Creators and owners of financial data (including individuals, businesses, entrepreneurs, small business, etc.).
- Permissioned Parties: Those who receive the data permissioned by consumers, generally for the purpose of providing the products, services, or insights that the consumer has requested (e.g. fintechs, lenders, personal financial management, applications, etc.).
- Data Aggregators: Organizations that act on behalf of the consumer to collect the consumer's data from financial institutions and provide it to Permissioned Parties.



- Financial Institutions: Institutions, like banks, whose primary function is to offer and provide financial services.
- Fintechs: Service providers that develop and utilize technology in connection with the provision of financial products, services, or insights.

It is important to note that "data brokers", who are typically not authorized or permissioned by consumers to collect, share, and/or use data, are not part of the consumer-permissioned financial data ecosystem.

Consumer-Permissioned Data

At the heart of this discussion is consumer-permissioned data. Consumer-permissioned data is data created by consumer financial activity (including banking, payroll, tax, insurance, and wealth/investment) and authorized or permissioned by the consumer for use in various applications or financial services. This data marks a critical shift in the financial services landscape. Historically, financial data was largely inaccessible to consumers apart from monthly paper or PDF-based account statements or pay statements. Over the past several years, however, innovation in technology has made it possible for consumers to access and consolidate statements electronically and to better understand their financial situation through personal financial management and budgeting tools. More recent innovations are now enabling consumers to "opt-in" their financial data to streamline the loan application process, gain access to new loan types or better loan terms, and even improve their generic credit scores.

Strengthening connections between consumers and third-party financial resources results in a more inclusive financial system and improves consumer financial wellbeing. These opportunities provide individuals and families across the socioeconomic spectrum with access to financial tools once reserved for the wealthy. Whether it's personal financial management tools, the ability to contribute data to credit scoring, or participating in peer-to-peer payment platforms, access to personal financial data changes lives.

5 Core Principles

Guidelines for Members of the Data-Sharing Ecosystem

Financial services centered on consumer-permissioned data have the potential to promote competition and to radically increase a consumer's financial stability, wellness, and inclusion. However, as with any innovation, it is imperative to build with an eye focused on goals and outcomes. Central to this building process are common standards and marketplace frameworks that certify processes and technologies. Fidelity, as a data access agent and insights provider, fully endorses in the core industry principles promoted by FDX: control, access, transparency, traceability, and security. Each of these intersect in critical ways; improvements in one area ripple across the others and result in enhanced processes and experiences across the board.



Control

Empowerment is meaningless without control. It is not enough to tell consumers that we have their best interests at heart. True empowerment rests on giving consumers control over how their data is used, who has access to their data, how frequently their data is accessed, and how long their data is retained.

Central to true control is informed consent. All ecosystem participants should provide consumers with intuitive navigation experiences presented in clear language. Too many steps, too much indecipherable fine print, and too many confusing processes inhibit informed consent and make things difficult for consumers.

One cornerstone of informed consent is a standardized permissions interface hosted by financial institutions. This interface allows consumers to easily view, modify, add, and revoke permissions across their library of financial services. When permissions are buried out of reach, consumers do not have the control they deserve. Power only exists when control can be exercised and managed.



Access

When it comes to financial data, the only acceptable level of consumer access is complete access. We believe that account ownership equals data ownership. Consumers' right to access personal financial data should (1) include the right to give a third-party permission to access it on their behalf and (2) mirror what they are able to see and access within their financial institution's web portal. This also includes having the same level of system availability and reliability when they've permissioned their data.

True accessibility means ease of use. Therefore, service providers should deliver a simple intuitive process for authentication that minimizes unnecessary steps and avoids language

that might cause confusion, delays, or abandonment. Time consuming or confusing digital experiences lead to lower rates of adoption. When consumers abandon a process for accessing their data because it does not meet their expectations, they may be missing out on beneficial services.



Transparency

As the owners of their financial data, consumers have a right to know exactly who will be accessing it and how it will be used. These important details can often get lost or skipped over due to overly complicated authentication processes. Market participants can increase transparency by using plain language and highlighting consumers' rights. Terms must also describe consumer options and the consequences of any available choices. We encourage businesses to find creative ways to incorporate these terms across the onboarding experience rather than reserving all terms and conditions for a lengthy document at the end of the consumer registration process.



Traceability

Traceability means that both consumers and permissioned parties should be able to map out the routes data takes along the data-sharing network. Each step, each transfer, each service provider should be clearly delineated. This mapping of the data-sharing flow also ensures that security breaches can be quickly and efficiently managed. In the event of a breach, all parties involved with the data in question should be automatically notified so that they can enact proper security protocols. A final facet of traceability is the right to be forgotten. This refers to an individual's right to require the deletion of all data that is not required to be held by law.



Security

Any discussion of industry standards and frameworks would be incomplete without careful consideration of security. All parties must have security policies and practices in place that a consumer would reasonably expect from a custodian of their sensitive data. This means constantly adjusting security measures to include advances in encryption and tokenization technologies. Security measures exist to protect consumers and should never be used as an impediment to consumers' ability to access their data.

Consumers are demanding the highest levels of data security. The number one reason customers abandon a transaction or interaction is because of a lack of visible security. Consumers need to be able to rely on market participants to provide clarity related to data definitions, usage, and privacy in order to make informed decisions related to the handling and privacy of their data. Investing in superior security measures drives every participant in the financial data ecosystem to deliver their very best and provides consumers the privacy and security they deserve.

By building their products on a foundation of these five core principles, participants in the financial services ecosystem also prepare for emerging data privacy regulations. When products are designed to emphasize consumer experiences of control, access, transparency, traceability, and security, integrating updated privacy guidelines and processes is simple. The groundwork is already in place to enable consumer-focused data privacy measures. In addition, some of these measures can be personalized for each user. Consumers should be able to elect the privacy levels and controls that work best for them. Privacy measures implemented within a consumer-centric framework deliver optimal personalization options.

Industry Collaboration

As described above, the financial data ecosystem is a complex web of interconnected and interdependent financial institutions, data access providers, fintechs, and users of consumer-permissioned data. All of these organizations must meet consumer demand and drive consumer-centric innovation if they want to succeed in today's marketplace. The Center for Financial Services Innovation states:

"Further coordination among all of the stakeholders in [data sharing] – 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."

It is exactly this complexity and connectedness that gives industry-led efforts the opportunity to promote standards and best practices that are as nimble and innovative as the industry they support.

In the financial data sharing ecosystem, FDX has emerged as a leader in standardizing financial data sharing, defining best practices, and driving industry adoption of the five core principles listed above.

FDX is a nonprofit collaboration of stakeholders dedicated to unifying the financial industry around a common, interoperable, royalty-free standard (the FDX API) and operating framework for the secure access of consumer-permissioned financial data. FDX aims to become a Bluetooth-like standards body for financial data so that consumers can securely access and share their data without needing to share or store their login credentials with third parties.

FDX is governed by a diverse Board of financial institutions, data aggregators, industry associations, and fintechs. It is actively involved in developing standards and best practices for consumer consent and permissioning. FDX is also the lead organization facilitating industry discussions that will guide security and certification standards that aim to decrease security risk within the ecosystem.

Simply put, Finity believes that FDX's industry-led effort is best positioned to address these obligations and challenges.

Regulatory Clarity & Modernization

Industry collaboration based on the five core principles of control, access, transparency, traceability, and security will ultimately provide the framework for an enhanced consumer-centric ecosystem of consumer-permissioned financial data. However, Finity's experience in the marketplace has revealed that key clarifications and modernizations related to regulatory oversight, as well as data ownership, privacy, and credit reporting regulations are needed. These reforms would support the five core principles and harmonize the otherwise splintered U.S. financial regulatory system in matters concerning consumer-permissioned financial data. Finity would welcome the opportunity to discuss the following reforms in greater detail:

- Regulatory coordination with respect to financial data oversight and enforcement.
- Clarifying and/or expanding consumers' right to access their data under Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act to give consumers (1) access to the full scope of their account and transaction data (i.e. access should include account owner information and routing number), and (2) the ability to authorize third parties to access and collect such data on their behalf.
- Clarifying and/or modernizing Fair Credit Reporting Act (FCRA) definitions, requirements and standards to account for the dynamics of consumer-permissioned data exchanges.

Finity also encourages regulatory agencies to enhance efforts that empower innovation within regulatory models. In sum, industry leaders and regulators should collaborate to create a safe and secure ecosystem where market participants can bring new products and services forward without undue fear related to unclear or overly burdensome regulations. Ultimately, unleashing consumers' financial data to their benefit will profoundly impact financial literacy, planning, and peace of mind.

About Us

Finicity is a data access and insights company based in Salt Lake City, Utah. Since our founding in 2000, we have worked to provide people with financial data that enables them to better understand and improve their financial health. To further that goal, we built financial data API connections to financial institutions and payroll providers that enable consumers to permission their data for use in third-party applications or solutions. Early in our history this meant enabling consumers to access their data in personal finance management and budget applications. Today it means consumers are able to use their personal financial data to speed up the process of getting a loan, verify and authenticate bank accounts for instant payments, manage their finances, and contribute data for a more accurate credit report and score.

Our years of experience have placed us at the forefront of the mortgage industry. We help to power the nation's largest lenders by providing the tools they need to simplify and digitize the origination process. As the only registered Consumer Reporting Agency in the data access and insights space, we uniquely empower consumers with dispute and disclosure procedures that are in compliance with the Fair Credit Reporting Act (FCRA) whenever their data is used for credit decisioning purposes.



The Honorable Stephen Lynch
Chairman
Task Force on Financial Technology
House Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC 20515

The Honorable Tom Emmer
Ranking Member
Task Force on Financial Technology
House Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC 20515

November 20, 2019

Dear Chairman Lynch and Ranking Member Emmer,

Plaid is grateful for the opportunity to comment on how consumer access to their financial data can improve their financial service choices. Plaid enables innovation in financial services by providing consumers access to and control over their financial data, and we support steps to establish rules that help consumers conveniently and safely use their financial information to improve their financial lives.

Every time a consumer receives a paycheck, buys something, makes an investment, or applies for a loan, they create a small amount of information about themselves. When consumers have control over the financial data they create, they can use it to better manage their financial lives. Consumers can use their data to build a budget, find affordable credit, send money to friends, monitor investments, and even share finances with significant others.

Unfortunately, in our current landscape much of this data is kept away from the consumers who produce it, stored by entities over which consumers have little influence. After years of lacking visibility into where and how such data was stored, manipulated, and sometimes even sold, consumers are now beginning to recognize the power that comes with control of their own data. This has led governments around the world, including the US, to explore what is referred to as "open banking." The simplest definition of open banking is a recognition of the consumer's right to access and use their own financial data to get products and services that best suit their needs.

Plaid connects one in four bank accounts in America with the fintech apps consumers want. Consumers want to be able to control their data and find products that meet their needs, banks want to maintain close relationships with their customers, and fintech companies want to be able to deliver the best products and services to consumers. The flow of secure data is critical to each of these groups, and Plaid has developed industry leading practices to ensure data security and privacy. We are supportive of efforts to establish rules that align the ecosystem around these standards.



While it's important for the FinTech Task Force to explore rulemaking to establish security and privacy safeguards for the flow of consumer financial data, it is essential that it also understand what companies are doing today to provide consumers the benefits of data access while protecting them from potential risk.

Consumers using Plaid are made completely aware and put in full control of what pieces of financial data are flowing, from which entity to which, and for what duration, and are able to instantly revoke access to their data. Further detail on Plaid's approach to consumer control can be found in the attached white paper, "Protect Consumer Control of Data to Build Trust." Importantly, we do not sell or rent end user information to marketers or other third parties. Plaid takes deliberate steps to protect consumer information in our possession. We maintain information security controls that are regularly evaluated for effectiveness against industry standards. We prioritize privacy and security, and have established standards that allow consumers to benefit from their financial data while keeping it safe.

Finally, any rulemaking around consumer financial data must begin with the recognition that consumers - not banks, aggregators, or third party providers - should be in control of their own financial data. Plaid is encouraged by this committee's recognition of the importance of Section 1033 of the Dodd-Frank Act, which recognizes consumers' right to access their financial information. We will continue to advocate for rulemaking around Section 1033 to ensure consumers stay at the center of the financial services system.

Plaid supports regulation that recognizes consumers' right to access and share their data, as well as the obligation of companies like Plaid to provide those consumers with the information and protections they need. We thank the committee for their close attention to this important issue.

Sincerely,

A handwritten signature in black ink, appearing to read "John Pitts", written over a horizontal line.

John Pitts
Plaid Policy Lead



November 20, 2019

Congressman Stephen F. Lynch
Task Force on Financial Technology
House Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC 20515

Congressman Tom Emmer
Task Force on Financial Technology
House Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC, 20515

Congressman Lynch and Congressman Emmer,

We applaud the Task Force on Financial Technology (“Task Force”) for holding this timely hearing on the role of technology and data practices at scale in financial services.

Digital technology, and the data that drives it, has provided numerous innovative products and services that have benefited the American public. Internet-related tech innovation has been so successful that consumers and users now rely heavily on internet services and platforms in nearly every facet of their daily lives. Despite the clear benefits, the pervasiveness of these services and platforms means there is the potential for significant harms that negatively affect users at scale.

When the personal data that fuels the online ecosystem is misused or abused, it can lead to a host of harms, ranging from physical and financial injury to lost opportunity to digital redlining. As Federal Trade Commission (“FTC”) Commissioner Rebecca Kelly Slaughter has noted, these harms disproportionately affect vulnerable and marginalized communities.¹ While such harms are well documented,² any advances in federal law to provide increased consumer protections have failed to keep pace. With no comprehensive federal privacy law in existence, there is no oversight, safeguards, or accountability for how companies collect, use, or protect the often-sensitive personal data they collect from internet users.

Further, a handful of platforms have established a level of dominance in various online services that raise serious competition concerns. These platforms appear poised to leverage existing dominance online to allow them to enter other markets, including financial services. In fact, some dominant platforms have already entered (or announced plans to enter) the space. The

¹ See Remarks of Commissioner Rebecca Kelly Slaughter, *The Near Future of U.S. Privacy Law*, Silicon Flatirons (Sept. 6, 2019), https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf.

² See, e.g., Public Knowledge Comments to the National Telecommunications and Information Administration, Docket No.: 180821780-8780-01 (Nov. 9, 2018), <https://www.publicknowledge.org/documents/public-knowledge-ntia-consumer-privacy-comments/>; Lawyers’ Committee for Civil Rights Under Law et al., *Letter to Congress on Civil Rights and Privacy* (April 19, 2019), <https://lawyerscommittee.org/wp-content/uploads/2019/04/Letter-to-Congress-on-Civil-Rights-and-Privacy-4-19-19.pdf>.

FTC, Department of Justice, and numerous Congressional committees are currently investigating potential competitive harms caused by dominant platforms and whether existing antitrust laws are sufficient to address dominance and market power in the digital economy. Several of these companies have also demonstrated carelessness or disregard for how they treat sensitive consumer data.³

Public Knowledge has long advocated for the importance of sector-specific regulation to protect consumers, promote competition, and further the public interest, including most recently in the context of dominant digital platforms.⁴ The Committee should be commended for its formation of the Task Force and for holding important hearings on financial technology data practices to build the public record and to identify ways to strengthen consumer protections in the financial sector. In this letter, we raise certain policy concerns that we identify in the digital platform space, particularly as it relates to financial services.

Privacy Concerns

Thousands of data brokering companies exist that collect thousands of data points on each individual in their data set, including highly sensitive information about health status and economic stability.⁵ For years, data brokers have operated in the shadows, free of meaningful government oversight, while they profit off of vast troves of consumer data. Because these brokers do not have a direct business relationship with consumers, they are often trafficking in personal data without consumer knowledge or consent. While some brokers offer consumer choices around how the broker may use personal data, the FTC has found a “fundamental lack of transparency about data broker industry practices.” The Senate Commerce Committee has reported that data brokers classify consumers in categories like “Ethnic Second-City Strugglers” and “Tough Start: Young Single Parents.”⁶ They can use these profiles to engage in harmful marketing practices like predatory lending and other digital redlining activities that disproportionately impact marginalized communities. Many data brokers are quite small, but some of these small entities are the most egregious privacy violators. For example, last year, Exactis, a data broker with only 10 employees was reported to have exposed the data of 230 million consumers.⁷ Government oversight of the data broker ecosystem is sorely needed to establish transparency and accountability and to protect user rights.

³ See, e.g., Federal Trade Commission, *FTC Approves \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, [ftc.gov](https://www.ftc.gov/news-events/press-releases/2019/08/ftc-approves-final-consent-order-settling-charges-background) (July 24, 2019), <https://www.ftc.gov/news-events/press-releases/2019/08/ftc-approves-final-consent-order-settling-charges-background>; Federal Trade Commission, *Privacy and Data Security Update: 2018*, <https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf>.

⁴ See generally, Harold Feld, *The Case for the Digital Platform Act: Market Structure and Regulation of Digital Platforms*, Roosevelt Institute (May 2019), <https://www.digitalplatformact.com/>.

⁵ See Aliya Ram and Madhumita Murgia, *Data Brokers: Regulators try to rein in the “privacy deathstars”*, Financial Times (Jan. 7, 2019), <https://www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521>. (Paywall).

⁶ See Committee on Commerce, Science, and Transportation, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes* (Dec. 18, 2013), <https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577>.

⁷ See Keri Paul, *What is Exactis—and how could it have leaked the data of nearly every American?*, MarketWatch (June 29, 2018), <https://www.marketwatch.com/story/what-is-exactisand-how-could-it-have-the-data-of-nearly-every-american-2018-06-28>.

As large tech companies like Apple and Facebook enter into the financial services market, more transparency and scrutiny is essential regarding the data that drives decisions by financial services providers. Companies are now using artificial intelligence technology based on deep machine learning to generate important decisions on creditworthiness. As was highlighted in an article earlier this year on Motherboard, companies like, “ZestFinance, Lenddo, SAS, Equifax, and Kreditech are selling their AI-powered systems to banks and other companies, to use for their own creditworthiness decisions.”⁸ These decisions, however, are not transparent, nor is it clear what data these companies are using in their deep learning AI to make credit decisions. Unlike other credit scores, there is no way to appeal these decisions, nor is it possible to learn the constituent parts that make up this new, secretive creditworthiness score.

Decisions on creditworthiness have been historically discriminatory against people of color, women, and members of the LGBTQ community. A recent paper highlighted the fact that as recently as 2018, face-to-face and fintech lenders charge, “otherwise-equivalent Latinx/African-American borrowers 7.9 (3.6) bps higher rates.”⁹ This recent data raises numerous concerns that are worthy of the Committee’s attention, including:

- What data is being used by these companies and how did they get it?
- How has the underlying data been tested, and have the requisite procedures been put into place to make sure that this data is not replicating historical inequities in the financial sector?
- What protections or means of appeal will be given to consumers to find out about secret credit scores and correct inaccuracies?
- Are the results that the machine learning AI is reaching explainable to the average consumer?

We urge the Task Force and the Committee to investigate whether the financial industry has thought of and instituted these necessary consumer protections.

Any privacy regime that Congress adopts to further protect user rights should not be based on data ownership. To the extent that data ownership even addresses the privacy problem—a tenuous connection—data ownership should not be grounded in copyright law, and new (sui generis) data ownership rights are likely to create practical and legal confusion that will not meaningfully protect consumer privacy. Privacy is a basic consumer protection issue best resolved through comprehensive federal privacy legislation. As discussed below, to achieve the worthy goal of data sharing to promote competition or scientific research, lawmakers should instead look at imposing data portability and interoperability mandates on certain online platforms to give users true choice and control over what to do with their data.

The asymmetric information and power imbalances that plague the current data ecosystem would persist under a data ownership regime. Individuals would not have the information to understand what they are selling, or the bargaining power to get a fair price. Aside from the

⁸ Rose Eveleth, *Credit Scores Could Soon Get Even Creepier and More Biased*, Motherboard (June 13, 2019), https://www.vice.com/en_us/article/zmpgp9/credit-scores-could-soon-get-even-creepier-and-more-biased.

⁹ Robert Bartlett et al., *Consumer-Lending Discrimination in the FinTech Era*, National Bureau of Economic Research, Working Paper No. 25943 (June 2019) <https://www.nber.org/papers/w25943>.

means of compensation, it's hard to see how this is any different from the current failed "notice and choice" privacy regime. Consumers already face the impossible task of reading and understanding¹⁰ countless opaque and lengthy privacy policies (read: contracts, often filled with legalese) that outline the scope of how their information is used by the companies that profit off of data, many of which we don't have any direct contact with. Note that individuals have zero leverage to negotiate these privacy policies and terms of use. This would not change under a data ownership regime.

In general, Congress should not create incentives for individuals to accept payment in exchange for signing over their personal data, which could include incredibly privacy-invasive information (such as biometric, health, and precise geolocation data) as well as seemingly non-sensitive information that could be used by trained algorithms to infer intimate information. Such arrangements could lead to disparate impacts affecting members of low-income and other marginalized communities who might not be so privileged to sell or lease their data sparingly. Pay-for-surveillance will surely be popular among data-hungry businesses. Companies have been willing to pay users, including teens, to collect user data,¹¹ and these companies have the leverage to change the terms of the contracts to the detriment of users at their whim. Congress should take steps to address this imbalance, not facilitate it.

Competition Concerns

Incumbent online platforms benefit from natural economic characteristics that protect their market dominance, causing a slew of competition policy concerns. Companies like Amazon and Facebook benefit from "network effects," meaning that as the number of users goes up, so do the benefits to users of being on the platform. In other words, all else equal, you benefit more from joining the social media platform your friends are on than you do by joining a newer or smaller social network without your friends. Many digital platforms benefit from economies of scale because their software has almost no marginal cost for adding users. Many digital platforms also benefit from economies of scope because data is much more valuable when aggregated and analyzed as a group instead of viewed as single pieces of information. If Google provides an individual's e-mail and maps, including traffic data, then Google can tell that individual when to leave for their flight so they arrive on time. By contrast, a competitor's mapping application that doesn't have access to the user's e-mail isn't even aware there is a flight to catch. Incumbent online platforms also benefit from behavioral ticks like "bounded rationality," where consumers use shortcuts rather than carefully choosing the best option each time. Most consumers don't check multiple online stores every time they buy oven mitts—they simply go to the same store each time. Similarly, users don't use Bing every few months to see how it matches up with Google's search engine—they just keep returning to Google Search.

The combination of these characteristics makes it incredibly difficult for small companies to grow and new companies to compete against incumbent dominant platforms. Without dynamic

¹⁰ See Kevin Littman Navarro, *We Read 150 Privacy Policies. They Were An Incomprehensible Disaster*, New York Times Opinion, (Accessed November 20, 2019), <https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html>.

¹¹ See Rachel Lerman, *Facebook launching app that pays users for data on app usage*, APNews (June 11, 2019), <https://apnews.com/289df88fb145472198e54024b5c2f6a8>.

competition, where new competitors actually pose a threat to the market position of incumbents, economists expect less innovation, higher prices, and lower product quality. Some harms are more obvious: less consumer choice and limited opportunity for entrepreneurship. The potential for these harms exists in the financial sector where incumbent platforms like Facebook and others have sought to expand their business into financial services. To the extent that dominant platforms have or plan to enter into the financial services market, we believe that the Task Force and the Committee should closely scrutinize the ways in which such arrangements can have anti-competitive effects.

An important tool that can be applied to promote competition in the digital platform space is interoperability. In simple terms, interoperability means enabling different systems and organizations to communicate with each other and work together. Interoperability achieves several interrelated benefits for consumers and the economy. First, interoperability gives consumers practical control over their personal data. Consumers should not feel stuck with a bad service because it has all of their data and their friends' data. Second, interoperability encourages innovation in both incumbents, who have to improve their services to keep users in the original platform, and challengers, who have a fighting chance to develop successful new products and services. Network effects can "lock-in" users—even when users are frustrated by a platform and would like to leave; users may be prevented from leaving due to the difficulties of switching to another platform and/or the network benefits of transacting with other users on the dominant service. To the extent that dominant platforms are operating in or are soon to enter the financial sector, the way in which they interoperate with competing services, like for example by disallowing competing forms of payment on a platform or network, should be closely scrutinized.

Conclusion

We urge the Task Force to investigate the privacy and competition concerns outlined above as you consider policies to address problems in the digital marketplace. Thank you again for your attention to these important issues.

Sincerely,

/s/ Dylan Gilbert
Dylan Gilbert
Policy Counsel
Public Knowledge

CC: Chairwoman Maxine Waters and Ranking Member Patrick McHenry

Question for the Record**Rep. French Hill****Task Force on Financial Technology****November 21, 2019 - Banking on Your Data: The Role of Big Data in Financial Services****Questions for Don Cardinal**

1. Mr. Cardinal, how many financial institutions have consumer data collected by data aggregators that are members of FDX?

Ensuring that consumers have access to their data and the ability to determine which financial data parties will have access to their data is a core principle within FDX's mission. As such, all financial institution members of FDX allow their customers to permission their own financial data for use with fintech applications either provided by a financial institution or through third party applications. Access to the data is typically provided by a data access provider (sometimes referred to as "data aggregators"). Further, it is likely that most financial institutions with online banking have data being accessed by data access providers based on public statements by the providers themselves on the number of firms they can potentially access. However, for anti-collusive purposes, FDX does not poll member firms to catalogue who has private contracts or bilateral agreements with whom.

- a. Of that universe, what is the number of financial institutions from which data is gathered via the FDX API?

Of FDX's 22 member firms that identify themselves as financial institutions, all of them have indicated that their FDX API implementation is in development, pre-production, associate pilot, pilot, or some phase of production. This was per an anonymous survey in Oct 2019 of member firms. Further, we estimate that eight (8) million U.S. consumers have been moved from data access using legacy technology (credential-based access and screen scraping) to next generation tokenized access via the FDX API to date.

- b. What is the number from which data is gathered via screen scraping?

To our knowledge, no firm is 100% migrated to APIs, so by definition, all firms are still utilizing legacy technologies to allow consumers to share their data. In addition, it is estimated that between 60-80 million US consumers have used or are using legacy technology today to permission their data with fintech applications that are provided by their own financial institutions or via third party applications and data access providers. This will remain the case until all data access provider and fintech access to a given financial institution is migrated fully to the FDX API.

- c. What is the number from which data is gathered via OFX?

Due to anti-collusive reasons, we cannot poll members for detailed business capabilities, even though OFX is now an independent working group supported by FDX. Given the size and tenure of the financial institutions that are FDX members, very likely almost all of them also offer OFX connectivity (either actively or have it as a legacy connection in containment). OFX has been in existence for over 20 years.

- d. What is the number from which data is gathered through other methods (please describe)?

Without knowing the detailed architecture of member firms, it is difficult to answer accurately. Data access methods could encompass several forms:

- i. API (FDX, another region's API, or a proprietary vendor API)
- ii. OFX (versions 1.0 through 2.2 offer slightly differing connectivity capabilities)
- iii. HTML scraping
- iv. Direct data feed (batch or real time)

2. Mr. Cardinal, what is the median time, from the start of negotiation to adoption, for each FDX member data aggregator to enter into an API agreement with a financial institution?

FDX is not privy to the legal and sourcing negotiations between member firms and has no data on the time needed for custom bilateral agreements. We have seen other industry groups take action in the area of bilateral agreements. The Clearing House (TCH), for example, has proposed a model bilateral agreement recently based on input from the top 25 U.S. financial institutions and several large fintechs.

See: <https://www.theclearinghouse.org/connected-banking/model-agreement>.

Questions for the Record

Hearing: “Banking on Your Data: The Role of Big Data in Financial Services”

Date of Hearing: November 21, 2019

Member: Rep. Ben McAdams

To Mr. Cardinal:

I know FDX is working on broad-based industry standards.

- Is the goal for that to be a system of bilateral agreements between a financial institution and a data aggregator or other fintech platform, or do you envision moving beyond that?
- Is moving beyond bilateral agreements necessary for scale and widespread adoption?

The Financial Data Exchange is a technical standards body whose mission is to unify the financial industry around a common, interoperable, royalty-free standard for secure and convenient consumer and business access to their financial data – namely the FDX API. Regarding bilateral agreements, for anti-collusive purposes, FDX is not involved, does not catalogue who has private contracts or bilateral agreements with whom and is not privy to the legal and sourcing negotiations between member firms. That said, FDX can provide some background on bilateral agreements.

Financial institution regulations require that if third parties are to be in receipt of a customer’s personal financial information and/or personally identifiable information, that strong governance be in place. Part of that governance is to clearly spell out the duties and obligations of each party to the other in matters of data security, fraud and risk policies, incident notification, and other areas. This is done in the form of an agreement between the parties – the data source and the data receiver.

At present, these relationships are being created via custom bilateral agreements. However, given the similarity of subjects in these contracts, it is likely that there will be a move over time to a common agreement as we have seen in other industries. In fact, The Clearing House (TCH) has proposed a model bilateral agreement recently based on input from the top 25 U.S. financial institutions and several large fintechs. See: <https://www.theclearinghouse.org/connected-banking/model-agreement>.

With respect to scale, we have seen approximately eight (8) million North American consumers converted off of the legacy technology (credential-based access and screen scraping) and onto next generation tokenized API based architecture, and expect to be at 12 million by April 2020. Further, the thousands of regional and community-based financial institutions and credit unions that are reliant on core technology providers to offer data access solutions to their customers will also have the capability once these core providers begin offering products and services utilizing tokenized API access. FDX is working to expedite this transition in a safe and prudent manner.

FDX seems focused on API standards development and adoption - whereas many of the early fintech apps used screen-scraping.

- Are there benefits to API versus screen-scraping for the consumer - either better data security, or more control on how to control and even revoke access?

You are correct. FDX's mission is to unify the financial industry around a common, interoperable, royalty-free API standard for secure and convenient consumer and business access to their financial data. However, this won't happen overnight and FDX acknowledges that time and flexibility are required to transition the consumer-permissioned financial data ecosystem away from credential-based access and screen scraping to tokenized access through the FDX API. The following includes some of the differences between credential-based access and screen scraping and tokenized, API-based access:

- With credential-based access and screen scraping, consumers provide their login credentials (e.g., passwords, challenge questions) to financial applications or data access companies which can then be used to access the appropriate financial institution and retrieve the consumer's data. Screen scraping retrieves data from an authenticated consumer via a permissioned fintech app or through a financial data access company (also known as a data aggregator) by logging on for the consumer and "reading" the content of the online banking web page. The retrieved data is then used and displayed in the consumer's chosen app or service.
- As a legacy technology, credential-based access and screen scraping have provided an essential avenue for consumers to use and share their own financial data. However, it is less efficient and effective than direct API access. Screen scraping also places stress on financial institution's tech infrastructure due to the sheer volume of automated logins. Finally, with screen scraping, the app or service permissioned by the consumer is able to read any data elements that are visible on the online banking web page.
- Tokenized access in concert with an application programming interface (API) takes a consumer to their financial institution during the app enrollment/sign-up process to log in with the consumers' financial institution, be authenticated and permission the data they would like to share. This replaces the need to provide their login credentials to an application provider or data access company. A token, or string of characters up to 1,000 characters long, is then generated and sent to the chosen application or data access company. This token replaces the consumer credentials and is then presented to the consumer's financial institution through an API. Put simply, an API provides a dedicated data portal where consumer-permissioned data is provided directly from a database containing the required data elements so that only the consumer's permissioned data will be shared with the application or data access company.
- Tokens contain no personally identifiable information, only work with the single financial institution the consumer uses and often expire in a short period of time. APIs make consumer-permissioned data sharing easier, more accurate and more secure. Not only do they remove credential sharing and provide a dedicated data access portal for data access providers and companies not affiliated with a consumer's financial institution, but they also lay out the rules for how to request data and what data will be returned.

In sum, any time fewer entities hold data, risk is reduced. As FDX removes the need to share consumer ID's and passwords with third parties, the risks of account take overs and other security breaches are decreased. This is a concept known as Data Minimization and the US Government through NIST (National Institute for Standards and Technology) calls this out. https://pages.nist.gov/800-63-3/sp800-63a/sec8_privacy.html

- And where will the industry move next?

While financial institutions and financial data access providers have moved approximately eight (8) million consumers to the FDX API as of January 2020, there are still an estimated 80 million consumers whose access and use of their data with fintech applications and financial data access providers is dependent on credential-based access and screen scraping. Further, until all data currently available via online or mobile banking access is available through a tokenized API connection, a complete transition cannot take place.

The introduction of chip cards (EMV) provides a helpful case study when considering the transition to tokenized API data access. EMV was a boon to consumer security when compared to cards featuring only magnetic strips, however it was not an overnight migration. In fact, while very large U.S. issuers started voluntarily issuing these cards in 2010, the full transition involved a staged implementation with non-EMV liability shifted to merchants in 2015, ATMs in 2016/2017 and gas stations in 2020. Finally, it is important to note that most small businesses were dependent entirely on their merchant services (terminal) provider for this conversion – not unlike the dependency today of regional and community-based banks and credit unions on core processors to adopt the FDX API.

FDX supports the transition from legacy technology (credential-based access and screen scraping) to next generation tokenized access via the FDX API. FDX is working to expedite this transition in a safe and prudent manner.

To all witnesses:

- Are there any recommendations for things the government could do to facilitate the move to APIs versus the practice of screen scraping?

The government is already actively involved, both regulators and lawmakers, in providing oversight and input. We simply ask that the door remain open for FDX and its member firms to brief you periodically on our progress and seek your advice and counsel.

We believe an industry-led initiative such as FDX offers the shortest critical path to realizing the benefits of secure, consumer-permissioned data sharing. In fact, other industries have successfully created Special Interest Groups to address such challenges. The Bluetooth Special Interest Group and the Mortgage Industry Standards and Maintenance Organization (MISMO) are good examples of the voices of industry coming together to successfully create a common standard. In sum, FDX anticipates that once its certification programs and procedures are established, widespread adoption of the FDX API as the industry standard will benefit consumers through consistent access to the data they need to make better financial decisions and improve their financial lives.

- Are there gaps between financial institution, fintech applications, and/or data aggregator practices and what consumers think is happening with their personal financial data?

FDX is committed to unifying the financial data ecosystem by empowering consumers through superior data control, access, transparency, traceability and security. All these core principles benefit the consumer's awareness and control over how they share their data. Further, as all players in the ecosystem adopt FDX standards, the consumer's experience in data sharing will be consistent among all parties.

- Do consumers understand for how long data may be stored or used after initial consent, and are there ways to improve consumers' understanding or control over the terms around data sharing?

The consumer consent flow for the FDX API describes how long the data access will be maintained. Other than for regulatory purposes, data minimization dictates that once data is no longer needed (*i.e.*, once a credit decision has been made, financial advice offered, credit score enhanced, or a tax return filed) it should be deleted.

One of the most useful ways to gauge customer understanding is to ask them. FDX has conducted several focus groups to ask consumers about the consent flow in terms of friction, understanding, comfort, and sense of privacy. Supplementing this design work, FDX has brought Consumer Reports and the National Consumer Law Center in as members with special focus on consumer consent and experience. We note their membership for informational purposes only and do not imply any endorsement by them of FDX or any of its work products.

Responses to Questions for the Record

Hearing: “Banking on Your Data: the Role of Big Data in Financial Services”

Date of Hearing: November 21, 2019

Member: Rep. Ben McAdams

Witness: Duane Pozza

Q: Are there any recommendations for things the government could do to facilitate the move to APIs versus the practice of screen scraping?

A: The Consumer Financial Protection Bureau (CFPB) has been looking closely at this issue and soliciting views from a range of stakeholders in connection with Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act. In 2016, it released a request for information on consumer rights to access financial account and account-related data, including an examination of market practices and potential market developments.¹ It also held a field hearing on consumer access to financial records.² The CFPB received a wide range of responses from stakeholders, including recommendations regarding potential further action by the CFPB, that can be found at <https://www.regulations.gov/docket?D=CFPB-2016-0048>. In 2017, the agency released Consumer Protection Principles on consumer-authorized financial data sharing, as well as a summary of stakeholder insights.³ Throughout this process, stakeholders have expressed a range of views as to what measures would be effective to advance the adoption of permissioned transfer of consumer financial data, which should be given further careful consideration. In general, consumers benefit from having a range of choices in financial services, including the ability to choose service providers in areas, like personal financial management, that rely on access to consumers’ financial data to provide beneficial services.

Q: Are there gaps between financial institution, fintech applications, and/or data aggregator practices and what consumers think is happening with their personal financial data?

- Do consumers understand for how long data may be stored or used after initial consent, and are there ways to improve consumers’ understanding or control over the terms around data sharing?

A: Different financial institutions and financial technology companies make different disclosures around their data practices, and it would be important to look at individual

¹ See Bureau of Consumer Financial Protection, *Request for Information Regarding Consumer Access to Financial Records*, No. CFPB-2016-0048 (Nov. 14, 2016), available at https://files.consumerfinance.gov/f/documents/112016_cfpb_Request_for_Information_Regarding_Consumer_Access_to_Financial_Records.pdf.

² More information can be found at <https://www.consumerfinance.gov/about-us/events/archive-past-events/field-hearing-consumer-access-financial-records-salt-lake-city-utah/>.

³ CFPB, *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation* (Oct. 18, 2017), available at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf; CFPB, *Consumer-authorized financial data sharing and aggregation* (Oct. 18, 2017), available at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf.

disclosures in assessing consumer understanding. In general, one potential source for determining whether consumers are encountering issues is the Consumer Sentinel Network (Sentinel), operated by the Federal Trade Commission (FTC). The FTC recently released its 2019 Consumer Sentinel Network Data Book summarizing consumer complaints in a range of categories, and can often provide more specific information.⁴ As I noted in my testimony, existing laws would apply in this area, including Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices. Under the FTC Act, deception involves a representation, omission or practice that is likely to mislead the consumer acting reasonably under the circumstances.⁵ This standard is applicable to companies making representations to consumers about how data – including financial data – is used and shared.

⁴ FTC, *2019 Consumer Sentinel Network Data Book* (Jan. 2020), available at https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf.

⁵ Letter from James C. Miller III, Chairman, FTC, to John D. Dingell, Chairman, Committee on Energy and Commerce, U.S. House of Representatives, (Oct. 14, 1983), available at https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf (FTC Policy Statement on Deception).



National
Consumer Law
Center

NATIONAL HEADQUARTERS
7 Winthrop Square, Boston, MA 02110
(617) 542-8010

WASHINGTON OFFICE
Spanogle Institute for Consumer Advocacy
1001 Connecticut Avenue, NW, Suite 510
Washington, DC 20036
(202) 452-6252

NCLC.ORG

January 27, 2020

Congressman Ben McAdams
Committee on Financial Services
Task Force on Financial Technology
U.S. House of Representatives
Washington, DC 20515

Re: Questions for the Record, Nov. 21, 2019 hearing on "Banking on Your Data: the Role of Big Data in Financial Services"

Dear Congressman McAdams,

Thank you for the opportunity to respond to your follow up questions regarding my testimony on November 21, 2019 on "Banking on Your Data: the Role of Big Data in Financial Services." My responses are as follows.

Q: Are there any recommendations for things the government could do to facilitate the move to APIs versus the practice of screen scraping?

Government should encourage industry players to work together to ensure safe ways of sharing data. While government should not require any particular form of technology, you should encourage companies to develop and use technologies that do not require sharing of usernames and passwords. The government should ensure that consumers' dispute rights under the Electronic Fund Transfer Act are respected no matter what form of technology is used in order to both protect consumers and provide incentives for safe methods of data sharing. The Consumer Financial Protection Bureau should begin supervision of the larger participants in the data aggregator market for consumer protection, privacy and security purposes. Congress also needs to require strong data security standards, along with examination and enforcement, for all parties that hold or use significant amounts of consumer data.

Q: Are there gaps between financial institution, fintech applications, and/or data aggregator practices and what consumers think is happening with their personal financial data? Do consumers understand for how long data may be stored or used after initial consent, and are there ways to improve consumers' understanding or control over the terms around data sharing?

Consumers do not know what is happening with their personal financial data. They do not understand how much data is accessed, what it is used for, who has access to it, or for how long. These are not issues that can be addressed through disclosures. Privacy policies are vague, the uses of data are complicated, privacy policies of different companies are intertwined, and policies can change.

Congressman Ben McAdams
January 27, 2020
Page 2

Disclosures or purported consent are not sufficient when data is used in ways that consumers would not reasonably expect. Congress should pass strong privacy rules, which do not preempt state law, that permit sharing of only the minimum amount of data that is needed consistent with consumers' reasonable expectations of the content, purpose, parties that have access, and time period of the sharing – consistent with the data sharing principles in my testimony.

Please let me know if you have any further questions. Thank you once again for inviting me to testify.

Yours very truly,

A handwritten signature in black ink, appearing to read "Lauren K. Saunders", with a long horizontal flourish extending to the right.

Lauren K. Saunders
Associate Director