

PRESERVING THE RIGHT OF CONSUMERS TO ACCESS PERSONAL FINANCIAL DATA

HYBRID HEARING

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

SEPTEMBER 21, 2021

Printed for the use of the Committee on Financial Services

Serial No. 117-46



U.S. GOVERNMENT PUBLISHING OFFICE

45-863 PDF

WASHINGTON : 2021

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	FRANK D. LUCAS, Oklahoma
GREGORY W. MEEKS, New York	BILL POSEY, Florida
DAVID SCOTT, Georgia	BLAINE LUETKEMEYER, Missouri
AL GREEN, Texas	BILL HUIZENGA, Michigan
EMANUEL CLEAVER, Missouri	ANN WAGNER, Missouri
ED PERLMUTTER, Colorado	ANDY BARR, Kentucky
JIM A. HIMES, Connecticut	ROGER WILLIAMS, Texas
BILL FOSTER, Illinois	FRENCH HILL, Arkansas
JOYCE BEATTY, Ohio	TOM EMMER, Minnesota
JUAN VARGAS, California	LEE M. ZELDIN, New York
JOSH GOTTHEIMER, New Jersey	BARRY LOUDERMILK, Georgia
VICENTE GONZALEZ, Texas	ALEXANDER X. MOONEY, West Virginia
AL LAWSON, Florida	WARREN DAVIDSON, Ohio
MICHAEL SAN NICOLAS, Guam	TED BUDD, North Carolina
CINDY AXNE, Iowa	DAVID KUSTOFF, Tennessee
SEAN CASTEN, Illinois	TREY HOLLINGSWORTH, Indiana
AYANNA PRESSLEY, Massachusetts	ANTHONY GONZALEZ, Ohio
RITCHIE TORRES, New York	JOHN ROSE, Tennessee
STEPHEN F. LYNCH, Massachusetts	BRYAN STEIL, Wisconsin
ALMA ADAMS, North Carolina	LANCE GOODEN, Texas
RASHIDA TLAIB, Michigan	WILLIAM TIMMONS, South Carolina
MADELEINE DEAN, Pennsylvania	VAN TAYLOR, Texas
ALEXANDRIA OCASIO-CORTEZ, New York	PETE SESSIONS, Texas
JESÚS “CHUY” GARCIA, Illinois	
SYLVIA GARCIA, Texas	
NIKEMA WILLIAMS, Georgia	
JAKE AUCHINCLOSS, Massachusetts	

CHARLA OUERTATANI, *Staff Director*

TASK FORCE ON FINANCIAL TECHNOLOGY

STEPHEN F. LYNCH, Massachusetts, *Chairman*

JIM A. HIMES, Connecticut
JOSH GOTTHEIMER, New Jersey
AL LAWSON, Florida
MICHAEL SAN NICOLAS, Guam
RITCHIE TORRES, New York
NIKEMA WILLIAMS, Georgia

WARREN DAVIDSON, Ohio, *Ranking
Member*
PETE SESSIONS, Texas
BLAINE LUETKEMEYER, Missouri
TOM EMMER, Minnesota
BRYAN STEIL, Wisconsin

CONTENTS

	Page
Hearing held on:	
September 21, 2021	1
Appendix:	
September 21, 2021	27

WITNESSES

TUESDAY, SEPTEMBER 21, 2021

Carpenter, Tom, Director, Public Affairs, Financial Data Exchange (FDX)	4
Carrillo, Raul, Associate Research Scholar, Yale Law School, and Deputy Director, Law and Political Economy Project	6
Cochran, Kelly Thompson, Deputy Director, FinRegLab	8
Smith, Steve, Co-Founder and CEO, Finicity	12
Wu, Chi Chi, Staff Attorney, National Consumer Law Center (NCLC)	10

APPENDIX

Prepared statements:	
Carpenter, Tom	28
Carrillo, Raul	47
Cochran, Kelly Thompson	67
Smith, Steve	83
Wu, Chi Chi	85

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Lynch, Hon. Stephen F.:	
Written statement of Acorns	99
Written statement of Akoya	102
Written statement of the American Bankers Association	106
Written statement of the Bank Policy Institute	119
Written statement of Envestnet Yodlee	123
Written statement of the Financial Data and Technology Association of North America	127
Written statement of the Financial Technology Association	135
Written statement of Pinwheel	138
Written statement of Plaid, Inc.	145
Written statement of The Clearing House	149
Williams, Hon. Nikema:	
Written responses to questions for the record submitted to Chi Chi Wu	172

PRESERVING THE RIGHT OF CONSUMERS TO ACCESS PERSONAL FINANCIAL DATA

Tuesday, September 21, 2021

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 10:03 a.m., in room 2128, Rayburn House Office Building, Hon. Stephen F. Lynch, [chairman of the task force] presiding.

Members present: Representatives Lynch, Himes, Gottheimer, Lawson, San Nicolas, Torres, Williams of Georgia; Davidson, Sessions, Luetkemeyer, Emmer, and Steil.

Ex officio present: Representative Waters.

Chairman LYNCH. Good morning. The Task Force on Financial Technology will 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 this task force are authorized to participate in today's hearing.

As a reminder, I ask all Members to keep themselves muted when they are not being recognized by the Chair. The staff has been instructed not to mute Members, except when a Member is not being recognized by the Chair and there is inadvertent background noise.

Members are also reminded that they may only participate in one remote proceeding at a time. If you are participating today, please keep your camera on, and if you choose to attend a different remote proceeding, please turn your camera off.

Today's hearing is entitled, "Preserving the Right of Consumers to Access Personal Financial Data."

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

Good morning, and welcome to this hearing of the Financial Services Committee's Financial Technology Task Force. Today's hearing will discuss various issues surrounding the gathering, usage, and protection of consumer financial data.

I would like to begin by thanking our distinguished panel of witnesses who have agreed to testify and offer their diverse perspectives as Congress and regulators grapple with the rapidly changing landscape in this area.

The collection and utilization of consumer financial data has exploded in the past decade as the usage of smart phones, myriad devicesx, and the Internet of Things, enhanced computational

power and algorithms, and artificial intelligence and robotic process automation have been combined to transform the way consumers manage their finances and conduct the most basic economic activities, while also changing the way financial services providers have responded to consumers' desires and preferences.

Whether using a payment processor to split a dinner bill, employing a personal financial management app to track spending, or accessing a mobile lending platform for a personal loan, consumers and financial services providers rely more keenly on the data flow that underpins the delivery of those services.

The consumer financial data ecosystem has also expanded beyond traditional banks and insurers to include data aggregators, payment processors, neobanks, and mobile lenders employing technologies that were not necessarily anticipated in earlier legislation and regulation.

While there is little doubt that recent emerging financial services innovations have real potential to improve the efficiency and accuracy of those services, while reducing costs and fostering greater inclusion, the relentless full spectrum cultivation of consumer data and the manipulation of that data raises important policy questions about personal data protections, user control, and meaningful consent to sharing that data, as well as the ultimate contours of personal privacy.

In fairness, many financial services providers, both traditional and Fintechs, have requested regulatory guidance and greater clarity in this area.

While some current laws governing financial data—the Gramm-Leach-Bliley Act, the Dodd-Frank Act, the Fair Credit Reporting Act, and the Equal Credit Opportunity Act—are generally instructive, there are serious gaps that leave much uncertainty, given the transformational technology and advancements as well as changing relationships and customer preferences that we face today.

Again, I want to thank our witnesses for your willingness to help the task force with this work. I look forward to our discussion.

And the Chair now recognizes the ranking member of the task force, the gentleman from Ohio, Mr. Davidson, for 5 minutes for an opening statement.

Mr. DAVIDSON. Thank you, Chairman Lynch.

I truly appreciate that you are conducting this hearing today on a very important and prevalent issue. Financial technology seems to be developing at the speed of light in recent years, so it is encouraging to see this task force and the committee keep up with the industry, or attempt to do so.

As I said 2 years ago when this task force held a similar hearing on personal financial data, it is great that there is common ground across the aisle on this topic. I think we all agree on the importance of protecting consumers' control over their own financial data.

But does this mean that we both, regulators and policymakers alike, are moving fast enough to address the uncertainties in this area? I am not convinced that we are.

However, it is encouraging to see the Consumer Financial Protection Bureau (CFPB) continuing to make progress towards a rule-making under Section 1033 of the Dodd-Frank Act. Section 1033

provides the opportunity to strengthen consumer control over their personal data. When a consumer grants consent for any party to access or hold their personal financial data, it is vital that this consent is read narrowly. I am optimistic that the CFPB can adequately define the proper scope of that consent.

Whether this involves limiting the specific financial activity for which the data is needed, or the length of time it is authorized, I expect these types of questions to be at the forefront of the CFPB's process as they undertake the rulemaking.

Ideally, they will conclude, as I have, that individuals have a property right to their own data, much like a songwriter would have protection for their lyrics or music as composed. Individuals own the data that they create.

As things currently stand, I believe that consumers do not fully appreciate what they are consenting to whenever they utilize third-party financial services providers.

Please note that this is not meant as a swipe at Fintech. Applying for personal loans, conducting peer-to-peer payments, getting mortgages, receiving financial product recommendations, just to name a few examples, has never been easier. Fintech companies have made financial services more accommodative than ever before.

Despite this financial revolution, we need better transparency regarding the relationships between financial institutions, third-party service providers, and the consumers who are providing the data.

It is encouraging to see some progress within the industry to shift away from practices such as screen scraping, which essentially circumvents any need for consent between a financial services provider and a third party, and towards application program interfaces.

However, I believe policymakers and regulators retain the authority to properly shape these relationships and protect consumers' financial privacy, moving forward.

I am not going to say that regulators need to impose regulations with technical guidance. It is best to leave those details to industry. However, regulators can still provide consumer-focused principle-based frameworks that will allow for innovation and competition.

I would be remiss if I didn't acknowledge that we have some industry-specific standards in place to address consumer privacy data. These policies can largely be found within the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Electronic Fund Transfer Act. While Section 1033 of the Dodd-Frank Act is a step in the right direction, we are left with a fragmented regulatory framework when it comes to consumer data privacy protection.

I know this hearing is more narrowly focused on the 1033 rulemaking and open banking, but I think it is important that Congress continues to hold the broader conversation as well.

We are in the process of developing a bill that will be called, "It's Your Data," which we hope will secure that property right in law for American citizens.

While we can all agree on the general outcome, reaching that outcome is a complicated endeavor through Congress. I am certain many questions here today will be rather specific and potentially complex.

Consumer data has become so leveraged and holds so much value that it has, ultimately, become a very large business asset. No matter how big the financial industry gets or how much financial technology evolves, the monetary value of consumer data will never be worth more than the fundamental right to privacy.

Our Constitution is supposed to protect the right to privacy for every American citizen, and it is our duty to do that.

I very much look forward to hearing our witnesses' testimony today, and I yield back.

Chairman LYNCH. The gentleman yields back.

Today, we are pleased to welcome the testimony of our distinguished witnesses: Mr. Tom Carpenter, the director of public affairs with the Financial Data Exchange; Mr. Raul Carrillo, an associate research scholar at Yale Law School, and the deputy director of the Law and Political Economy Project; Ms. Kelly Thompson Cochran, the deputy director of FinRegLab; Ms. Chi Chi Wu, a staff attorney with the National Consumer Law Center; and Mr. Steve Smith, the CEO and co-founder of Finicity.

Witnesses are reminded that their oral testimony will be limited to 5 minutes. You should be able to see a timer on your screen that will indicate how much time you have left, and a chime will go off at the end of your time. I would ask that you be mindful of the timer, and quickly wrap up your testimony if you hear the chime, so that we can be respectful of both the witnesses' and the committee members' time.

And without objection, your written statements will be made a part of the record.

Mr. Carpenter, you are now recognized for a 5-minute summation of your written testimony.

Thank you.

STATEMENT OF TOM CARPENTER, DIRECTOR OF PUBLIC AFFAIRS, FINANCIAL DATA EXCHANGE (FDX)

Mr. CARPENTER. Thank you.

Chairman Lynch, Ranking Member Davidson, and members of the Task Force on Financial Technology, thank you for the opportunity to testify at today's hearing.

My name is Tom Carpenter, and I serve as director of public affairs at the Financial Data Exchange, or FDX. I must begin by saying that FDX is currently barred from taking positions on most legislative or regulatory policy issues. FDX does advocate for market-led API standards for data sharing.

Please consider the rest of my comments today as educational and intended to inform the task force about FDX and the way that our work interacts with policy and legislation.

The best analog to understand FDX is the Bluetooth standard. As consumers now know today, Bluetooth brought together many different consumer electronics manufacturers to create standard specifications so that consumers could use differently branded products in an interoperable manner.

In the same way, FDX brings together diverse financial industry players under a common application programming interface (API) standard. This allows consumers to share and move financial data between financial institutions, Fintechs, and intermediaries in a se-

cure and transparent manner, and one which is not dependent on where one banks or which Fintech app a consumer may choose to use.

And most importantly, adoption of the FDX API is replacing the need for data sharing that relies on shared consumer login credentials and screen scraping.

A few additional details about FDX. FDX is a nonprofit body. The FDX API is also royalty-free. FDX currently has 200 members across the financial sector globally, including Fintechs, banks, data aggregators, consumer groups, payment networks, financial industry groups, and other stakeholders, and I am pleased to be joined in this hearing at the witness table by Chi Chi Wu and Steve Smith, who both represent FDX member organizations.

And in case you thought FDX was just an interesting concept, I am pleased to tell you that 22 million consumer accounts have been transitioned from screen scraping to the FDX API so far. That is 22 million consumer accounts.

As this task force is aware, Fintech innovations are allowing consumers to use their own financial data to lower costs, for more efficient processes, better rates, and lower fees, expanding credit access to thin-file or no-file borrowers when a traditional credit score is limited or incomplete, and to empower better decision-making via a consumer's own big data, just like large companies have done for years, so they can actually see all of their accounts in one place.

With this in mind, here are a few key points I would like to make the task force aware of today.

First, it is critical for the task force and regulators to draw a bright-line distinction between user permission financial data sharing versus data brokerage or data harvesting.

Consumer permission data sharing, all data sharing using the FDX API is fully controlled by the consumer and must include explicit consumer consent. Data brokers or harvesters instead collect and sell data about consumers, often without expressed consumer consent, control, or awareness.

Second, FDX is committed to and believes that five core principles must be present in any system of financial data sharing or open banking to ensure the industry serves the needs of consumers.

These principles are control, access, transparency, traceability, and security. I expand upon these in my written testimony, and I would be happy to answer any questions about them.

Third, FDX believes that technical API standards are best left to the financial industry rather than defined by regulators.

For a host of reasons and, again, expanded upon in my written testimony, we believe the industry is best suited to maintain and continually adapt standards to the needs of the market and consumer demand.

As for the potential CFPB rulemaking, FDX submitted comments to the CFPB's Advance Notice of Proposed Rulemaking (ANPR) earlier this year, and FDX was actually mentioned or referenced in almost half of the comments the CFPB received.

As above, our comments stressed to the CFPB the importance of FDX's five principles, as well as our core belief that technical data-sharing standards should be left to the industry.

FDX also believes a potential CFPB rulemaking would need to find a good balance. Consumers must be able to access and share the full extent of their own financial data with third parties via APIs in the same way they can today via screen scraping, including some third parties who may have no relationship with a consumer's data provider.

At the same time, data providers like banks must be able to maintain sound risk management practices and activities consistent with applicable laws and regulations. FDX is hopeful that its own certification of FDX API implementations will be helpful here.

Finally, FDX encourages the CFPB to do more to prioritize the adoption of market-led API standards, and to reference or acknowledge these standards to further amplify the work and also to harmonize industry standards and regulation as much as possible so the standards are not caught between competing or overlapping or disjointed requirements.

Thank you again for the opportunity to testify today.

[The prepared statement of Mr. Carpenter can be found on page 28 of the appendix.]

Chairman LYNCH. Thank you, Mr. Carpenter.

Mr. Carrillo, you are now recognized for 5 minutes to give an oral presentation of your testimony.

STATEMENT OF RAUL CARRILLO, ASSOCIATE RESEARCH SCHOLAR, YALE LAW SCHOOL, AND DEPUTY DIRECTOR, LAW AND POLITICAL ECONOMY PROJECT

Mr. CARRILLO. Thank you.

Chairman Lynch, Ranking Member Davidson, and distinguished members of the task force, thank you for inviting me to testify this morning.

I offer my testimony as an associate research scholar at Yale Law School, but I previously worked as an attorney for low-end consumers in New York City, and as special counsel to the enforcement director of the CFPB.

This morning, I repeat previous calls for policymakers to adopt a bright-line approach to financial data regulation, recognizing both the benefits and harms of collecting highly personal information.

Today, a payment made with a mobile money account typically includes a merchant, bank, payments processor, mobile device maker, internet service provider, and an app provider.

Additionally, roughly, 50 percent of U.S. consumers and 95 percent of U.S. deposit accounts are estimated to have signed up for financial apps that frequently rely on unregulated or underregulated data aggregators. All of these companies can share data widely with other corporations and law enforcement agencies. I agree with the National Consumer Law Center that consumers deserve more control over their data relative to banks and other financial institutions.

That being said, consumer rights to access, review, manage, correct, and delete data can only be meaningful with a broader policy that minimizes data collection and inappropriate usage as a first-order principle.

Although we should be able to entrust Fintechs and aggregators to collect data on our behalf, this collection process itself must be subject to greater accountability. Section 1033 rulemaking should promote consumer control of information but in the broader context of data minimization, rather than maximization.

Just as the CFPB offers more control to consumers via their agents using technologies like APIs, they must enforce Federal consumer protection, including fair credit reporting laws, in this space.

If consumers are harmed, and either banks, Fintechs, or aggregators have not provided accurate records of existing financial information and, just as importantly, not included an explanation of how account data has been shared, the CFPB should take appropriate action with the presumption that noncompliance with Section 1033 rulemaking has led to unfairness to consumers and the broader purpose of Dodd-Frank, with which the CFPB was entrusted, has not been upheld.

Beyond this, we must upgrade Federal consumer data and privacy and security laws from the notice and consent paradigm. There are limits to the ways in which individual consumers can meaningfully make choices about how their personal data is used.

As legal scholar Salome Viljoen argues, the very point of data protection in the digital economy is to put people into population-based relations with one another and predict broader trends in social and collective behavior.

Corporate and government actors frequently do not even know the purpose of collection until after they analyze an aggregated data set and identify proxies.

Meaningful consent cannot exist when people do not know what information they are reviewing or to what end. As a matter of public policy then, we should not be able to forfeit our general rights to data privacy and security simply by clicking, “agree,” as industry would often have us believe.

Ultimately, Congress must shift the burden of data protection from consumers, courts, and litigators to regulators and tech companies. The collusion of big tech and Wall Street in this space and the continuing blurring of distinctions between financial and non-financial data demand especially careful scrutiny.

Legislation should limit processing to only the minimum amount of data strictly necessary to carry out an explicit narrow purpose, such as the provision of a good or service requested by individuals, and then intentional interaction. This principle itself demands a robust form of transparency that Section 1033 rulemaking can help provide.

I agree with Ranking Member Davidson’s earlier comment that privacy concerns should trump property concerns in this space. Privacy and security are especially important as we consider policies of financial inclusion into poor communities and communities of color.

People may volunteer payments and credit data that, when aggregated, confers sensitive information about disadvantaged groups in unpredictable ways. Public benefits, family, criminal, immigration, and national security law already provide a channel for policing troubled by civil rights concerns that is further exacerbated by surveillance.

Moreover, mass data collection does not solve our deeper issues of financial exclusion. Apps are solutions to certain problems, acute problems, but not structural problems.

The erosion of data security and privacy law and consumer finance should encourage us to move away from overreliance on credit as a method of social provisioning, growth, and poverty reduction, and focus on better jobs, higher incomes, and more equitable economic policies.

Thank you.

[The prepared statement of Mr. Carrillo can be found on page 47 of the appendix.]

Chairman LYNCH. Thank you, Mr. Carrillo.

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

**STATEMENT OF KELLY THOMPSON COCHRAN, DEPUTY
DIRECTOR, FINREGLAB**

MS. COCHRAN. Good morning, and thank you again to Chairman Lynch, Ranking Member Davidson, and the members of the task force.

My name is Kelly Thompson Cochran. I am the deputy director of FinRegLab, an independent research organization that evaluates the use of data and technology to create a more responsible and inclusive financial marketplace.

We have published a number of reports on customer data access issues, including a groundbreaking evaluation—empirical evaluation—of the use of cash flow data for underwriting small business and consumer credit.

Our research finds that the system for consumer-directed transfers is benefiting many consumers and small businesses today, but it is also creating risks and burdens that reduce its ability to create greater customer-friendly innovation and competition.

Efforts to meet the financial services needs of underserved populations may be particularly sensitive to these risks and burdens, for instance, where providers' margins are already thin, or particular populations are particularly sensitive to concerns about privacy and data security.

Thus, improving the market and regulatory infrastructure for customer-directed transfers has critical implications for competition, customer protection, and financial inclusion, going forward.

We are encouraged to see several Federal regulators beginning initiatives to address critical threshold issues. While additional work by industry and Congress will be needed to improve the broader data ecosystem, the regulatory initiatives are critical to help sharpen the focus of these complementary efforts.

The market today is moving towards more safer and more efficient technologies for data transfers, both through bilateral agreements between large players and through broader standardization initiatives.

But progress has been slowed by competitive tensions, coordination challenges, and regulatory uncertainty. While industry-led standardization efforts can be highly beneficial, particularly on technical issues that are hard to enshrine in regulation, historical

experience suggests that such efforts will be far more efficient and effective if regulators set certain basic parameters.

Three such initiatives are currently underway. In addition to the CFPB's 1033 rulemaking, which we have already discussed, the Federal Trade Commission is modernizing information security standards for nonbank financial services providers under the Gramm-Leach-Bliley Act, and prudential regulators are harmonizing third-party service provider guidance as it applies to customer information data transfers.

We believe that the industry efforts will be substantially strengthened if the regulators address five key sets of issues in their proceedings.

First, the deadline for particular groups of financial service providers to make data available upon consumer request under 1033.

Second, the scope of the data that is subject to 1033 data access rights, the application of exceptions to that statute, and whether financial data sources can impose additional conditions on data transfers.

Third, the obligations of companies that are acting on behalf of a consumer in connection with a 1033 data transfer and the requirements for data recipients to safeguard that information.

Fourth, the CFPB's plans to begin supervision of data aggregators and other nonbank financial service providers that compile large amounts of customer permission data.

And fifth, the scope of banks' oversight responsibilities concerning aggregators or aggregators' customers in their downstream handling of customer data.

Interagency coordination is critical between these various initiatives because they are deeply interconnected. For instance, CFPB's supervision of aggregators could reduce third-party risks to banks, and third-party service provider guidance can affect the technical infrastructure and processes for 1033 data transfers.

These regulatory initiatives will also help to pinpoint the need for specific congressional actions. For instance, 1033 does not affirmatively define protections for data transferred under its provisions, and while other Federal laws potentially provide safeguards, they were not crafted specifically for this transfer system and may not apply to all of its use cases.

More broadly, as others have discussed, there are other gaps showing up in the financial regulatory ecosystem as players and data practices and technologies change.

Our written testimony discusses this in more depth, things like meaningful consumer permission while also dealing with the fact that there is evidence of customer overload, information overload, in trying to manage all of the permissions with which they are faced.

The CFPB and other Federal agencies will likely grapple with many of these cross-cutting issues in the course of these proceedings. But Congress has a critical role to play in creating consistency across statutes.

Modernizing customer data protections would help to reduce risk to consumers and small businesses, create a more level playing field among financial services providers, and encourage greater innovation and competition, going forward.

Thank you again for the opportunity to speak today.
 [The prepared statement of Ms. Cochran can be found on page 67 of the appendix.]

Chairman LYNCH. Thank you very much.

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

**STATEMENT OF CHI CHI WU, STAFF ATTORNEY, NATIONAL
 CONSUMER LAW CENTER (NCLC)**

Ms. WU. Thank you. Thank you, Mr. Chairman, Ranking Member Davidson, and members of the task force for the opportunity to testify. I am testifying on behalf of the low-income clients of the National Consumer Law Center.

The topic of this hearing is preserving the right of consumers to access personal financial data, and I absolutely agree. We support the President's Executive Order on competition and its call for the CFPB to continue the Section 1033 rulemaking.

Access to personal financial data, in particular bank account transaction data, has a lot of potential to benefit consumers. In particular, it could benefit the 45 million credit-invisible consumers who lack a credit history or have a file so skimpy that a credit score can't be generated.

But any access to personal financial data must be subject to what I call, "the three Cs and one D": consumer choice and control, competition, and consumer protection; and the "D" is data security.

Think about the data that is being accessed, how sensitive and revealing it is. Think about your own bank statements or credit card statements, and remember, a lot of credit-invisible consumers won't have a credit card so they will be using their debit card a lot.

Bank account transaction data might show when the consumer gets paid, where they shop, what advocacy organizations they support, or which health care providers they use.

So, consumers need control. Consumers are tired of not having control over our own personal data. We are tired of tech giants silently collecting data about us to show creepy personalized ads, and the original privacy-invading tech giants are the big three credit bureaus—Experian, Equifax, and TransUnion—which started collecting our information and monetizing it over 50 years ago without our permission.

We need a better system with strong provisions for consumer control, not just whether it is consented sharing, but for what purposes, for how long, and control over exactly what data elements get shared.

And no mice-type, click-wrap, pro-forma consent. It must be real, meaningful, informed, and knowing. Dashboards such as the ones developed by FDX are a good start. What is not good are efforts to access bank account data without consumer control, which, unfortunately, we are starting to see, including a current pilot for this company called Early Warning Services, to supply bank account information without consumer consent.

Competition. After the Equifax data breach, there was a lot of discussion about how consumers have no control over credit bureaus because we are not the customers; we are the commodity.

And it is true. The credit reporting system is an oligopoly, really a functional monopoly where we can't choose between the big three or walk away.

Data aggregators and financial account data could serve as potential competition to the credit bureaus, and it could be more accurate precisely because of consumer control. If an aggregator does a terrible job with the accuracy of data, consumers should have the ability to revoke consent and delete their data from the aggregator's database.

Of course, one risk we are already beginning to see is that the big three have started purchasing alternative data providers. For example, all three have bought consumer reporting agencies specializing in subprime credit. We would be really worried if the big three started buying up data aggregators as well.

Consumer protection. New entrants to a market love to claim they are the best thing since sliced bread and existing regulation doesn't apply to them because they are so innovative or novel. But, not so much.

Even though they were drafted several decades ago, the Federal consumer laws were written pretty broadly. So if it is used for credit underwriting, the Fair Credit Reporting Act applies and the Equal Credit Opportunity Act is implicated. And since deposit accounts are involved, the Electronic Fund Transfer Act is implicated.

I very much appreciate that my fellow witness, Finicity, has taken a similar position with respect to the Fair Credit Reporting Act.

In addition, we have urged, as part of the Section 1033 rulemaking, that the CFPB should establish supervision authority over larger participant data aggregators.

Data security. Speaking of supervision, we need supervision for data security. Since the Equifax data breach in 2017, we have urged Congress to transfer the data security authority in Gramm-Leach-Bliley to the CFPB for credit bureaus, and we would urge the same with respect to data aggregators.

At a minimum, the FTC should complete its rulemaking to strengthen the safeguards rule under that Act. Financial account information holds great promise, but also great risk. It could open doors to credit from millions of underserved Americans.

But the nightmare scenario is a system where every consumer, thick or thin file, high FICO score or not, is forced to give up their privacy and allow each creditor, employer, insurer, landlord, and government agency a direct and permanent digital pipeline to their bank account data.

It is up to the regulators and, ultimately, Congress to make sure that this data promotes consumer welfare without hurting our interests.

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

[The prepared statement of Ms. Wu can be found on page 85 of the appendix.]

Chairman LYNCH. Thank you, Ms. Wu.

And Mr. Smith, you are now recognized for 5 minutes for a summation of your written testimony. Thank you.

**STATEMENT OF STEVE SMITH, CO-FOUNDER AND CEO,
FINICITY**

Mr. SMITH. Thank you. I would like to thank Chairwoman Waters, Ranking Member McHenry, Chairman Lynch, Ranking Member Davidson, and the FinTech Task Force for the opportunity to speak with all of you today.

My name is Steve Smith, and I am the co-founder and CEO of Finicity, a MasterCard company. Finicity allows financial account holders, typically consumers and small and midsize businesses, to easily connect their accounts to a wide range of financial apps and services.

This is often called, “data aggregation.” I spent the past 30 years working in the technology industry. In that time, there has been remarkable technological innovation. From the internet to mobility to cloud computing, we have experienced massive advancements impacting virtually every industry.

One notable technology disruption has been the use of data and analytics. Large enterprises have leveraged powerful data and analytics tools to gain insights on business operations, improve efficiency, enhance consumer experiences, and much more.

All of this has enabled significant cost reductions combined with enhanced revenue opportunities. For too long, we, as individuals, families, and small and midsize businesses have not reaped the same benefits of using our data.

Why? The technology has been too expensive or the ability to collect and analyze our data has been exceptionally difficult or cumbersome. This is where the advent of open banking or open finance powered by data aggregation is flipping the data experience to one that empowers consumers and small and midsize businesses with access control and the consented use of their data.

Open banking is enabling a wide range of financial products and services that are transforming how consumers manage their money, prepare their taxes, apply for loans, make real-time payments, and better understand and improve their credit.

All of this is leading to more consumer choices and better experiences, along with increased financial literacy, financial inclusion, and improved financial fitness.

Finicity has been at the center of many of these empowering experiences. For example, we have enabled consumers to contribute more data to their credit scores through Experian Boost and through the UltraFICO score. These solutions use cash flow data explicitly permissioned by users to help them build or improve credit and achieve their financial goals.

So with all of this positive movement, why am I here? This is a technological shift that is still very much in the early innings. As it emerges and matures, Federal policymakers will play a meaningful role in the direction and pace of this transformation by providing clarity on data protection expectations, data privacy requirements, and consumer data rights.

Clearly, consumer data protection is a must throughout the data access and sharing process. Safeguarding the data is foundational to accelerating innovation while protecting the consumers from data theft.

Equally, I believe we all agree that the privacy of personally identifiable information is important to further consumer empowerment. In many respects, data privacy is about consent.

With clear and explicit consent, consumers will know where, how, and for what purpose their data is being used. Putting them in control enhances privacy. Data should not be shared across or among organizations without direct and transparent consent.

Finally, and I think, most importantly, consumer data rights must start and end with an individual's ability to access, use, and benefit from their data. This is foundational to open banking.

It is essential that consumers have reasonable access to all of their financial data in possession of the data holders in a format that they can permission for use in financial services and app providers of their choosing.

It is critical to safeguard data rights. Otherwise, the great progress we have made so far will fade. Data rights, privacy, and protection are an [inaudible] policy goals, each deserving focus and critical thinking.

Trade-offs may have to be made to balance competing objectives. Even adopting newer and better technologies can have unintended consequences by curtailing data access. We should bear in mind that these three goals are not equal. The consumers' right to their data must always be prioritized and maintained.

We need a clear regulatory framework to protect and continue open banking in the United States. That is why we are encouraged by the CFPB finally moving forward on a rulemaking under Section 1033 of the Dodd-Frank Act.

When we started Finicity, we started with one simple thought: Data is the heart of good decision-making. It is incumbent upon all involved in this data-sharing ecosystem that consumers in small and midsize businesses are empowered with the data they need to make the best decisions for themselves, their families, and their organizations.

Thank you again for the opportunity to address the task force, and I would be happy to answer any questions you may have.

[The prepared statement of Mr. Smith can be found on page 83 of the appendix.]

Chairman LYNCH. Thank you, Mr. Smith.

I now yield 5 minutes to myself for questions.

Let me ask the entire panel this, although I will select individuals at various times. The General Data Protection Regulation (GDPR) in the European Union has indicated that they have done it from a general policy approach.

They have recognized the right to be informed, the right to access data by individuals, the right to rectification if there is a flaw or a mistaken statement there, the right to restrict processing, the right to portability so that it encourages competition that an individual can move their data, and also the right to erasure or the right to be forgotten, so-called.

From a policy perspective, did they get that right, Ms. Wu? Have they gotten it right or are there gaps in what we have seen them attempt to accomplish?

Ms. WU. Thank you, Congressman Lynch, for the question.

Many of the principles in the GDPR are reflective of fair information principles and, in fact, some of them are reflected in the Fair Credit Reporting Act. Some of them were adopted in California with their consumer privacy law.

The devil is always in the details. When you talk about principles-based regulation, you want to drill down to the details. But, in general, GDPR has put in place a stronger framework than exists in the United States and has served as a model, as you can see, for some States.

Chairman LYNCH. Thank you.

Mr. Carpenter, what are your thoughts? You are trying to develop this uniform standard on APIs. Would your suggested structure embrace those rights that have been articulated in the GDPR?

Mr. CARPENTER. Thank you, Chairman Lynch.

I think a couple of things are at play. Technical API standards defined by the industry will always be subservient to any regulatory or policy actions that are put in place. So, whatever the industry defines, that the CFPB or other regulators define as principles or specifics, then standards will meet those obligations as needed.

I think it is important to think a little bit about the complexity of the U.S. market as compared to the EU or some of the other countries that have gone with a strong regulatory model for open banking or data sharing.

A lot of those countries have a single financial regulator. We have a myriad of them, a lot of times with overlapping jurisdiction in these areas. A lot of those countries also have—the financial services industry is held by just a few banks. We have well over 10,000 financial institutions in this country.

I think the U.S. is unique in its complexity and there will need to be a balance between what the regulators do as well as what the industry does.

So, I can't comment specifically on exactly what regulators should do or where that dividing line is. But we typically look at open banking as a, "how," and a, "what."

The, "what," is really up to regulators and policymakers. The, "how," is how is this accomplished? How does data move from point A to point B? And that is what we think is best left to the industry.

Chairman LYNCH. Thank you.

Ms. Cochran?

Ms. COCHRAN. I think that the GDPR framework is extremely helpful in the sense of thinking through the elements that need to be decided in, really, creating robust consumer and small business control over their own data.

But the exact policy balancing depends on the particular use case that you are doing. For instance, we have really focused on credit, which I think is one of the hardest cases, because while the existing credit information system—traditional credit bureaus—often don't require consumer consent to access data, the new system under 1033 does.

That creates an opportunity to create a much more robust system where consumers have more control over what is happening. At the same time, you have to balance that against the need of creditors to be able to access representative historical data so that they can

develop models that are fair and predictive and do a good job for both the customer and the lender.

So, balancing both the individual rights and the public interests are complicated. GDPR is really helpful because it starts to think through those questions, although I think often that the balance may be different for particular use cases in particular situations.

Chairman LYNCH. Doesn't much depend on consent? Meaningful, real consent?

Ms. COCHRAN. Yes. That is one of the things that I didn't get much time to talk about in my main testimony.

A lot of our system today in the U.S. does depend on notice and consent to data activities, but it is kind of a take-it-or-leave-it process. And what GDPR does is a much more robust thought process about how can consent be revoked, can data be deleted, and other questions.

Thinking about consent is more than a one-time transaction. But we also know that there is a great deal of evidence that consumers are already overloaded by the decisions they are being asked to make, and by the notices they are being asked to read.

One of the things that I think GDPR is struggling with and that would come up as the U.S. looks at this is how do you make some of those decisions simpler so that consumers can really focus on the critical things that they need to decide, and strip away some of the surrounding things that may be more secondary, could be more consistent, and then make the decision more meaningful and more powerful, in addition to those rights.

Chairman LYNCH. Thank you.

The Chair now yields to the ranking member of the task force, the gentleman from Ohio, Mr. Davidson, for 5 minutes for his questions.

Mr. DAVIDSON. I thank the chairman. And I thank our witnesses. I appreciate not only your verbal testimony but the written testimony as well and the preparation you have done for this hearing.

Mr. Smith, a November 2019 survey by The Clearing House found that 80 percent of financial app users were not aware that apps may use third parties to access consumer financial information.

From your personal experience, can you speak to the progress that has been made within the Fintech industry that would improve customers' awareness of how their financial data is being used?

Mr. SMITH. Yes. Thank you very much.

With respect to the issues surrounding consent and knowledge of consent, a lot of progress has been made. Finicity, for example, makes it very clear that Finicity is a services provider in the middle of the consented process between the consumer and the financial institution or financial services provider that holds their data.

They see the FDX organization has also put in place a working group and has promoted standards, UI standards, that make it very clear how to use consent or how to apply consent in a best-practices format that also makes very clear the players that are involved in that.

And then I would just say that Finicity, together with several others in the industry, both data holders and technology providers,

has started implementing at-pace dashboards that allow consumers to understand who is involved in the consent process.

Mr. DAVIDSON. Yes. Thank you for that, and for just highlighting the user-friendliness.

Ms. Cochran, your testimony in particular highlighted the consumer-friendly nature that is really so important. A lot of times, people will say in industry, in particular, well, it is in our terms and conditions, and if you print it out, it is 400 pages in a 6-point font, and sure, you just acknowledged it.

Could you elaborate on that, and how we could do this? I will come to you next, Mr. Carpenter, because of some of the things you have both dealt with deal with how GDPR is being applied versus, really, our inaction in America on privacy.

Ms. COCHRAN. Yes. There is some academic research that I think suggests that consumers would have to spend 25 days a year reading all of the disclosures that they get on digital data across all sectors, not just financial services. But it is really incredible.

Clearly, we need to get much crisper about and much more customer-friendly about the disclosures that are being done to make them really effective just in time, adapted to digital formats. A lot of people are reading things over their phones and really thinking through those questions.

At the same time, as I said before, we also need to think about how many questions are we asking consumers to answer in one shot, and do you divide those into maybe smaller chunks to give consumers more control as they think through their process and different questions at different times?

So, there is a real challenge ahead. The CFPB has disclosure authority that can be really helpful in this space. Consumer testing, obviously, is going to be hugely important. I think there are already some industry efforts that are moving in that direction.

But we know that there is this broader question about overload that is really one of the biggest challenges in this space is to make that meaningful and manageable and quick, in a way that is helpful to consumers.

Mr. DAVIDSON. Yes. Thank you. And I think you also touched on the fact that some things just have to be off the table because none of us want to use an interface that is just a relentless series of pop-up ads.

It is a tactic. It is not actually a real consent or choice for consumers.

Mr. Carpenter, one concept, I think, that is key to the discussion is the idea of data minimization or the idea that companies should collect minimal data to provide the product or service.

On the other hand, many businesses collect data that is not directly tied to providing the service and, of course, they want to use it maybe someday in the future, perhaps even for resale. Who knows? There is no end to the amount of data that some companies want to collect.

Mr. Smith, you made that reference that there are trade-offs. But I was really pleased that you concluded that we are never—the Fourth Amendment is not for sale, another bill that we are going to try to deal with in a bipartisan way.

Could you touch on how to strike that balance and where regulators can help do that?

Mr. SMITH. Yes, thank you, Congressman Davidson.

I would say, first of all, on data minimization, it is something that FDX is looking at in terms of defining and, really, APIs as opposed to screen scraping, provide far more consumer control over your data sharing.

With screen scraping, you are sharing everything you can see, and with APIs, you do have the ability to potentially limit data that you share for a given purpose.

We have internal use cases that are used for certification on the back end to ensure that the implementation of an FDX API is actually certifiable.

The question is, what can we do on the consumer front end to possibly provide that? So, that is an area that we are looking into.

I will say, just to touch on your prior question as well, awareness is one of our five principles, consumer awareness, and we are defining user experience.

And per the other witnesses' testimony, we are looking at it both on the front end—what does the enrollment look like, how many screens does it take before a consumer just drops out, because there are too many questions—but then also, through these dashboards. So, it is not just a one-time awareness but an ongoing awareness.

Mr. DAVIDSON. Thank you for that. My time has expired. I yield back.

Chairman LYNCH. The gentleman yields back.

The Chair now recognizes the gentleman from New York, Mr. Torres, for 5 minutes.

Mr. TORRES. Thank you, Mr. Chairman.

I have a real concern that the biggest banks, in opposing a Section 1033 rulemaking, are stifling competition and choice under the guise of consumer protection and cybersecurity.

There are, to be sure, legitimate cybersecurity concerns surrounding the consumer-authorized use of data. But it seems to me those concerns are best addressed not by allowing the big banks to hoard financial information for themselves but by regulating data aggregators and by protecting consumers.

I disagree with Mr. Carpenter's earlier statement that the standard should be left to the industry because the big banks are not disinterested arbiters of what is best for consumers.

The banks do have a vested interest in maintaining their oligopoly on consumer information.

So my first question is to Ms. Wu and Ms. Cochran. Is it fair to say that the big banks have a conflict of interest and, therefore, cannot be trusted to make disinterested determinations about what data to share, when to share it, and with whom to share it?

Ms. WU. Thank you for the question, Representative.

Certainly, consumer advocates are very concerned about ensuring that consumers do have the ability to share the data when they have a meaningful opportunity to consent.

One of the things that banks early on used as a tactic to try to prevent data sharing is to tell consumers, if you share this data via

screen scraping and there is some sort of unauthorized use, you will be on the hook, which we thought was just terrible.

The last person who should suffer a loss if there is some sort of data breach or unauthorized access is the consumer themselves, and we thought that Regulation E didn't allow for that, and, fortunately, the CFPB, in a recent FAQ, took that position as well. It is not the consumer who is going to suffer the loss.

So we do think that a 1033 rulemaking needs to go forward, and we are encouraged that there has been more cooperation. But, ultimately, I think there needs to be some regulatory teeth, especially if we are going to get rid of screen scraping because we can't get rid of screen scraping, until we have the ability for consumers at all banks to share the data, and that is not going to happen until you have these agreements with all institutions.

Ms. COCHRAN. I would just add a couple of thoughts.

As I said in my main testimony, there are competitive tensions all over this market—both banks and nonbanks—and they intersect in very complicated ways.

I think it is one of the reasons why it is so important for the regulators to set certain parameters to settle certain questions so that industry can focus on then implementing in an efficient way that actually benefits everyone once those decisions are made.

The other thing that I think is really important here is the inter-agency coordination that I talked about, because concerns about liability are legitimate open questions in this marketplace that affect everyone, and getting better answers to those questions and getting better answers to third-party service obligations, for instance, intersect with competitive interests.

So if we can settle the regulatory questions, that kind of decouples these dynamics that can feed on each other in ways that tend to slow the process of the overall system and reduce the benefits for innovation and competition that Section 1033 potentially offers.

Mr. TORRES. Thank you.

And I certainly agree that there should be regulation. As I said, there are legitimate concerns about cybersecurity and there is a legitimate concern that data regulators are, largely, unregulated and unsupervised.

I guess my question is for Mr. Smith. I am curious to know your obligations as a data aggregator. Do you have an obligation to provide accurate data and to correct inaccuracies and errors in data? Do you have a legal obligation to do so?

Mr. SMITH. As an aggregator, we also maintain a Community Reinvestment Act (CRA) status and are regulated under the Fair Credit Reporting Act (FCRA). We also have signed a number of bilateral agreements with leading financial institutions that require us to maintain compliance to certain aspects of the Gramm-Leach-Bliley Act (GLBA), and we maintain compliance to both State and Federal consumer privacy regulations today and also maintain compliance to GLBA.

So, that is the scope of the regulatory framework that we fall under.

Mr. TORRES. And I have a question for Mr. Carpenter. I am concerned about screen scraping because it involves the use of login

credentials. What is the timeline, in your opinion, for a full transition to API?

Mr. CARPENTER. That is a great question. I wish I had a clear answer to give to you. I think you have to think about the fact that, and Ms. Cochran talked about this a little bit and Ms. Wu did as well, there is a long tail in the United States.

And so, while the biggest financial institutions who usually invest in their own technology stock are quickly able to move to APIs, a lot of the community financial institutions or minority-owned financial institutions usually use a technology core provider, so they are waiting for that core provider to give API access or to, essentially, level the playing field across all of the financial institutions.

So, I would just say bringing the core providers in, and we have several that are members of FDX, to ensure that there is not a gap between the large and the small will help that timeline get accomplished.

But I think with any technology transition—we often talk about the chip card—the magnetic stripe, the chip card transition. There were a lot of different waypoints along the way that had to be accomplished before you could declare success.

Mr. TORRES. My time has expired. Thank you.

Chairman LYNCH. The gentleman from New York yields back.

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

Mr. LUETKEMEYER. Thank you, Mr. Chairman, and thank you to all of our witnesses today.

This is an interesting discussion we are having here. Whenever I discuss screen scraping with my constituents and explain to them what it is, they are aghast. They are absolutely horrified that when they give an okay to a third party to—or to their utility company to direct draft off their bank account, they wind up with a third party having access to their account. They are absolutely horrified that this is happening.

So, why do we allow that? Why do we not have a separate agreement which says that if you are going to be able to screen scrape and take that information and sell it, then the individual has to have a separate agreement with the different company, or with a company that is going to have a separate agreement with them that allows them to do that and then pay them for that information? Why is that not a viable option?

Mr. Carpenter?

Mr. CARPENTER. Thank you, Congressman Luetkemeyer.

I think it is helpful to think about the context of screen scraping. It is an old technology. It is not a perfect technology. It has a lot of issues.

It is also what has delivered the innovation that we have today in the competitive financial services market, and I would argue that without the ability for a consumer to access and share their own data via screen scraping, again, while not perfect, we would not have had the explosion in competition in the financial services industry.

Mr. LUETKEMEYER. Yes, but Mr. Carpenter, let's be honest here. This is all done without the consumer's knowledge. Most of your consumers, I will guarantee you—Mr. Smith, you made a comment

a while ago that 84 percent of people didn't know what was going on or they didn't approve of who had access to their information.

Mr. SMITH. Yes, I think that was referring to a TCH survey from 2 years ago.

Mr. LUETKEMEYER. But most people don't approve of what you are doing. They don't approve of screen scraping. We are sitting here making the assumption that everybody thinks it is okay. I am telling you that people don't believe it is okay and, therefore, we need to take a different perspective on this and say, whoa.

The first way you protect people's privacy and their information is to be honest with them up front, and say, this is what is happening with your information and how people are accessing it, unbeknownst to you.

We are approaching this from the wrong angle, I think. If people want to allow their accounts to be screen scraped, that is fine. That is an individual decision. They want to be able to have other people, other companies, have access to it so they can prevent, and with other options and other services. That is fine.

But most people do not know what is going on and would be very reluctant to sign a form that says it is okay to do that. So my question is, why can't we do that? Why can't we have the company be honest with them up front and sign a separate, completely different form—yes, I understand, Ms. Cochran, we are going to have another screen you have to go through and sign off on something.

But this should be in bright red letters, a whole new screen that says when you sign this agreement you are going to give access to the screen scrapers of the world to go with this, and this has to be something completely different than having a third party be able to have access to your account to make payments for you.

Mr. CARPENTER. Congressman, that is exactly what we are doing as fast as we possibly can to move to an API realm where instead of giving your login credentials, you are actually being taken to your financial data provider or financial institution, you are logging in, you are permissioning your data there at your bank on your mobile app. You are then being handed back with a token or a key so that an API does completely circumvent the sharing of login credentials.

So, the industry is rapidly moving in that direction. As I mentioned, 22 million consumers have currently been transitioned to the FDX API. It is just a matter of, it does take time. You can't flip that switch overnight and cut off access to the consumer data sharing that they have, and I think we are also working—

Mr. LUETKEMEYER. Whoa, whoa, whoa. Mr. Carpenter?

Mr. CARPENTER. Yes, sir?

Mr. LUETKEMEYER. You missed my whole point by your last comment. People aren't aware that this is going on. Why are you allowing it to continue? Shouldn't we as Congress, or the CFPB as a regulator, say, whoa, people are not aware that this is going on?

They should be told. There should be options presented to them. Why can't that be done right now? Why is this allowed to continue to go on, when we know that people don't know what is going on?

Mr. CARPENTER. And I would just say—

Ms. WU. Congressman, if I may, this is one area where we completely agree. You and I are on the same page. We think that this

sort of mice-type consent is not acceptable. We need meaningful, informed, separate dashboard, separate web page consent. And not just a yes or no, but how much information to share and for how long.

I understand the concern about information overload. It is something we are worried about, too, and how you design the consent is very important and that is something that FDX and others are working on, so that it is easy.

But yes, a yes/no decision would be easy, would prevent overload, but it wouldn't maximize the control, and we think the consumer should have maximum control over their own data.

Mr. LUETKEMEYER. I see my time is expired, Mr. Chairman. I yield back. Thank you.

Chairman LYNCH. The gentleman yields back.

The Chair is very pleased to welcome the Chair of the full Financial Services Committee, the gentlelady from California, Chairwoman WATERS, for 5 minutes.

Chairwoman WATERS. Thank you so very much, Mr. Lynch. I certainly appreciate this hearing. It is very important. And it seems as if I am agreeing with Mr. Luetkemeyer for the first time since we have served on this committee together.

Mr. LUETKEMEYER. Isn't that an overwhelming feeling, Madam Chairwoman?

Chairwoman WATERS. I want to make sure, and this may have been discussed before I came in, but I want to know about opt-out as opposed to opt-in. I get, from the people I do business with, something in small writing on page 15 somewhere, that says, if you want to opt-out, you have to let us know.

And people don't pay any attention to that. They don't even know what is meant by it. And if you don't opt-out, your information is shared with a third party, the third party shares the information with somebody else, somebody else shares the information, and then you get all these solicitations, people who are not only soliciting you for their products, and we don't know anything about those firms, and what protections we have, et cetera.

So, this is very simple to me. Mr. Luetkemeyer asked, why don't we just change it, why don't we just make sure the consumer knows? He talked about it a little bit differently, but my question is very simple: Why don't we just change the law, or make a law that says you cannot simply offer to opt-out on page 31, and if you don't do it, your information is going to be shared?

Mr. Carpenter?

Mr. CARPENTER. Yes, ma'am. Madam Chairwoman, thank you for the question. I want to be very clear up front that I am not in any way sticking up for screen scraping in its current manner. Our entire organization's mission is to move to a new API standard.

In terms of your question, everything that happens through consumer permission data sharing is directed. It is that opt-in, as you say, directed by the consumer. They are the one who downloads the app to start with. They are the one who goes to their financial institution to permission their data. So, none of what we are doing with FDX is taking a consumer's data without permission or consent.

Chairwoman WATERS. Ms. Cochran?

Ms. COCHRAN. Yes. I think this is an incredibly important issue, and it cuts across 1033, Gramm-Leach-Bliley, and the Fair Credit Reporting Act. Right now, we have Federal laws that don't require consent at all. They just set permissible purposes and say companies can use it within those bounds. We have laws that rely on opt-out consent, which means the data flows unless the consumer says no. And now, with 1033, we have a regime where the consumer has to say yes to turn it off.

So, we have all three in our current system. We know consumers are overloaded with the choices they are making. And so the balance between both how do we do sent well, where consumers really understand and are making the decisions they intend to make, and how do we, in some cases, maybe define the permissible purposes so they don't have to decide everything on a company-by-company or product-by-product basis. That is why this is so complicated, and it really requires looking more broadly, even beyond the 1033, to get to the answers to some of these questions.

Chairwoman WATERS. And what is your recommendation?

Ms. COCHRAN. There is a lot of evidence that opt-out consent is very sticky, that consumers don't tend to see it, they may not be reading those regimes. And so, I think that one in the middle is a particularly tricky category. We know, in GDPR and some other jurisdictions, that people are starting to look harder at purposeful purpose regulations so that consumers don't have to decide everything, or that there are gradations and tiers to how many things that they are asked to decide quickly in one setting. And I think looking closer at both of those options is potentially really helpful.

Chairwoman WATERS. I want to be very clear that on the opt-out opportunity, if you do nothing, that means that you opted in, is that correct?

Ms. COCHRAN. Right.

Chairwoman WATERS. Something is wrong with that. Thank you. I yield back the balance of my time.

Chairman LYNCH. Madam Chairwoman, I am going to yield to Mr. Carrillo to ask him to offer his observations on this.

Mr. CARRILLO. Thank you very much. Thank you very much, Chairman Lynch, and thank you for the question, Chairwoman Waters. I think that permissible purpose regulation is necessary at this point and we need to go beyond the notice and consent paradigm. It is possible, within notice and consent laws, to allow for click-wrap contracts, as the National Consumer Law Center has noted, that give companies the ability to harvest data based on the agreements, but data that is far more than what was intended by the consumer.

So, the agreement between the consumer and a company is not the appropriate site of regulation. We need to establish a longer list of how companies can use data, and to what end. There are still tricky questions as to intent, but it is a better frame to look at this from a broader perspective of public policy rather than identifying what consumers understand or not at the point of sale or point of agreement. Thank you.

Chairman LYNCH. I thank the gentleman.

The Chair now recognizes the gentlewoman from Georgia, Ms. Williams, who is also the Vice Chair of our Subcommittee on Oversight and Investigations, for 5 minutes.

Ms. WILLIAMS OF GEORGIA. Thank you, Mr. Chairman. Thank you for holding this hearing today for this important task force.

Anyone who follows my work in Congress knows that closing the racial wealth gap, which in my home of Atlanta, unfortunately is the worst in the nation, is the goal that I infuse into all of my policy work, especially my work here on the Financial Services Committee. In Congress, we have to be sure that financial innovation proceeds in a way that doesn't just deliver benefits to a few but to all, especially those most marginalized.

Today, I would like to focus on how we ensure personal consumer data is not used to reinforce racial and other biases. The discussions that we have here and the policy that we pursue will determine the level of progress that we make toward building an economy that is inclusive and fair for all.

Ms. Wu, in your testimony you mentioned that we need to be looking out for and preventing disparate impact when it comes to data used for credit purposes. Could you elaborate on what best practices Congress can employ to make sure that we're picking up on any broad patterns of disparate impact? How can Congress be sure we are addressing any issues through legislation as needed, and making sure that the CFPB and other agencies are writing appropriate and timely rules of the road?

Ms. WU. Thank you for the question, Congresswoman Williams. Certainly whenever big datasets are used, whether it's new data, like cash flow information, or old-fashioned data, like credit reports, one of the things that you really want to look for is racial disparities and disparate impact. We know, as a baseline, that credit reports and credit scores exhibit huge racial disparities.

Cash flow information and the work by FinRegLab shows that it may be more promising as a source of information, but it is still going to show racial disparities. Why? For a number of reasons. First, it still reflects fundamental underlying racial disparities in economics in our society, and second, overdrafts. Cash flow information will never truly be able to benefit consumers of color until we get rid of overdraft abuses, because that is one of the key things that they look for in cash flows, and we know overdrafts hit minority consumers a lot harder. We have to deal with the overdraft abuses.

With respect to big datasets and artificial intelligence and machine learning, one of the things we have seen is that they are not free of racial disparities. They reflect back what exists. If you take a dataset that inherently has racial disparities, and you have the AI or machine-learning model learn from it, it is just going to replicate it. And the problem is, people think, oh, AI and machine learning, there is no bias, but there is. It is all a reflection of the underlying data that is a reflection of the inequalities in our society.

And so, we need to be cognizant of that. We need to be aware of that. The unequal position of African Americans and Latinx consumers in this society was built from decades and centuries of intentional discrimination, and we are not going to deal with those

disparities until we intentionally try to address them consciously. If you just say, let's treat everyone equal, that is not equity and that is not going to do it.

Ms. WILLIAMS OF GEORGIA. Ms. Wu, you just mentioned that Black consumers are desperately impacted by bank overdraft practices, and that we should keep this in mind when related to consumer data, to whom consumer data is employed. So, how could greater use of no-fee accounts address the underlying disparity informing the data, going forward? Can you tell us the importance of simultaneously addressing concerns with the data used and disparities that inform the data being used?

Ms. WU. Certainly, there have been a lot of efforts to provide bank accounts for folks who have struggled with overdrafts, accounts that don't impose overdrafts and overdraft fees, that don't allow people to overdraft with their debit cards, which is a huge problem, that don't reorder transactions. And efforts by organizations to promote banking are very helpful. And you can't get cash flow bank account information if you don't even have a bank account, and we know there are also disparities on who has a bank account. And we know that lots of consumers, low-income and minority consumers are driven out of the banking system by overdraft abuses.

So yes, efforts to get unbanked consumers into bank accounts that are low-fee and safe are really important, but what is really more important is congressional action to just tamp down on those overdraft abuses and make sure that they do not hit all consumers, not just the ones who are able to benefit from no-fee and safe bank accounts.

Ms. WILLIAMS OF GEORGIA. Thank you, Ms. Wu. I am out of time, Mr. Chairman, but I do have another question around technology and broadband access that I will submit for the record, and hope that one of our esteemed panelists can provide some answers on that as we continue to move forward in this work.

Thank you, and I yield back.

Chairman LYNCH. I thank the gentlelady, and we welcome her question.

The Chair now recognizes the gentleman from Wisconsin, Mr. Steil, for 5 minutes.

Mr. STEIL. Thank you very much, Mr. Chairman. I would like to dive in, Mr. Carpenter, if I can, with you. In your testimony, you talked about the, "what," and the, "how," of open banking. I thought it was well said, the, "what," being the question of which data fields are shared and under what agreements or restrictions, and the, "how," more of the technological question.

I think another really appropriate question for us, and I would love to have you speak to it, is what is the appropriate role of the Federal Government in helping to address those two questions that you posed?

Mr. CARPENTER. It is a good question. I wish that I had the perfect dividing line for you. I tried to set it up. I think what has happened in the U.S. is many will say, oh, the U.S. is so behind in open banking. The truth is, we are actually in front. If you look at the number of consumers who have access to their data, and the ability to use it in innovative Fintech services, we are actually

leading the world in that regard. And so, I would argue that the CFPB and other regulators have actually taken an appropriate time to watch the industry mature in this area.

That said, where there are friction points, the Federal Government may need to step in to decide some of these issues. Industry standards can do a lot, but we are not a silver bullet. We cannot answer every single sticky policy question. I think where the government might see friction between the industry or the inability to come to a decision on, say, the scope of data or the like, it may be a role for the Federal Government to step in.

Mr. STEIL. Thank you. Mr. Smith, I would like to hear your thoughts on the same thing. Hearing kind of his take, could you give us any thoughts as to what the appropriate role is for the Federal Government?

Mr. SMITH. Yes. I think when you take a look at some of the conflicting aspects of this, as I spoke to in my oral testimony, you often run into situations where underregulation of financial institutions are, and rightly so, very concerned and very focused on safety and soundness. Safety and soundness gives way to data security, data privacy, gives way to limitations on the types of data that might be accessible.

So, when you look at rights to access, regulation would be helpful, clarity would be helpful to determine the types of data and scope of data that can be accessed for particular use cases, for example.

These are the kinds of things that, as a data aggregator—and I would just say, we’ve been leading the industry and signing bilateral agreements with financial institutions. By the end of this year, we will have greater than 60 percent of our data, 60 percent of the data flowing through our access pipes, integrations, through API integrations, that use a lot—there is an authentication methodology and do not collect credentials. And we further will have, in the pipeline, another 20 percent of the market coverage in integration development.

And so, these are some of the key issues with which we deal.

Mr. STEIL. Let me build on that a little bit, because I think in your written testimony you comment on some other countries and their open banking policies, and I want to get back to Mr. Carpenter as well on the same question. Looking at what other governments have done as far as government intervention in the private market in this space, what lessons have been learned about the appropriate role of government regulation in this space?

Mr. SMITH. Yes, I think Mr. Carpenter’s comment was that the U.S. has certainly been leading from an innovation perspective and has more of a wait-and-see attitude from a regulatory perspective, where other countries have been a bit more aggressive or proactive, from a regulatory perspective.

Mr. STEIL. And knowing that they have been more aggressive or more proactive, your term, what do you think the lesson learned is from that?

Mr. SMITH. Yes, I think there is a benefit to understanding what the use case and the value proposition is to consumers and forming regulation around ensuring that consumers are not harmed in any

way and that the value proposition associated with open access to data is maintained.

Mr. STEIL. Okay. Let me jump back to you, Mr. Carpenter, on the same topic. What lessons learned do you see from government intervention, in particular in foreign countries?

Mr. CARPENTER. I would argue that the lesson learned is that you can't really go with all one approach or the other. There really does probably need to be a hybrid approach. When you have an entirely regulatory-dictated system, you end up with compliance versus actually meeting the needs of the market.

What standards are able to do is actually follow the consumer: Where is the demand? Where does the market actually need definition and standardization? It doesn't mean that there may not be room for principles-based regulation or regulation or government action that solves some tough questions. So, I would argue that what we have seen is that you probably do need a little bit of a mix of everything.

Mr. STEIL. Thank you very much. I apologize that with the time, we couldn't get to all of the witnesses. I yield back.

Chairman LYNCH. The gentleman yields back.

Well, together with the ranking member, the gentleman from Ohio, Mr. Davidson, I would like to thank our witnesses for their testimony today.

The Chair notes that some Members may have additional questions for these witnesses, 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.

This hearing is now adjourned. Thank you.

[Whereupon, at 11:21 a.m., the hearing was adjourned.]

A P P E N D I X

September 21, 2021



Testimony of Tom Carpenter

Director of Public Affairs, Financial Data Exchange (FDX)

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

**Hearing entitled “Preserving the Right of Consumers to Access Personal
Financial Data”**

Tuesday September 21, 2021
Rayburn House Office Building, Room 2128

Chairwoman Waters, Ranking Member McHenry, Chairman Lynch, Ranking Member Davidson, and Members of the Task Force on Financial Technology, thank you for the opportunity to testify at today’s hearing. My name is Tom Carpenter and I serve as the Director of Public Affairs for the Financial Data Exchange (FDX).

FDX is an international, nonprofit organization operating in the US and Canada that is dedicated to unifying the financial industry around a common, interoperable, royalty-free standard for the secure and convenient access of permissioned consumer and business financial data, aptly named the FDX Application Programming Interface (FDX API). FDX is currently comprised of over 200 data recipients like fintech companies, data providers like financial institutions, and data access platforms like data aggregators, as well as consumer groups, payment networks, financial industry groups and other stakeholders in the user-permissioned financial data ecosystem. FDX is an independent subsidiary of the Financial Services Information Sharing and Analysis Center (FS-ISAC).

In essence, FDX operates as a Bluetooth-like specification to enable API-based financial data sharing with fintech services. Just like Bluetooth, FDX has brought together diverse financial industry players from banks to fintechs, data aggregators to consumer groups, payment networks to industry associations and many stakeholders in between to define a common API standard so that the financial industry is not fragmented into a maze of proprietary standards. Just like Bluetooth offers consumers the ability to use different consumer electronic products in an interoperable manner, regardless of manufacturer, FDX is defining a common standard so that sharing and moving financial data between financial institutions, fintechs and intermediaries is seamless, secure, transparent, consumer centric, and not dependent on where one banks or which fintech app they choose to use. And most importantly, through implementation of the FDX API, users within the financial data ecosystem are able to be securely authenticated without the sharing or storing of their login credentials with third parties. In fact, through broad adoption of the FDX API, screen scraping, or the retrieval of financial account information

with a user's provided login credentials, will eventually come to an end, and the flow of user-permissioned data between banks, aggregators, fintech applications, payments, and online lending, for example, will be more secure and reliable.

The good news today is that FDX is not just an attempt at such industry standardization and transition to API-based financial data sharing. Rather, and less than three years since its founding, FDX is a roaring success. FDX has surpassed 200 members that all work through FDX's over 30 different working groups and task forces to continue developing and enhancing the FDX standards. The FDX API itself is being implemented broadly across the financial services industry and will soon be certified for required data elements, technical conformance and availability. The FDX API is currently used by 22 million consumer accounts in the US and Canada for financial data sharing. Further, the FDX API currently defines over 620 unique financial data elements that consumers can access, share and leverage for their own financial benefit, making it one of the most robust open finance APIs in the world today.

Scope of Testimony:

My testimony today is drawn from the insight and perspective FDX has gained as an industry standards body with diverse membership¹ across the financial services ecosystem. In this, my hope is to provide the Task Force with a vantagepoint into the relationships between financial data providers² (i.e., financial institutions and banking organizations), data recipients³ (i.e., third-party financial technology companies or fintechs) and data access platforms⁴ (i.e., data aggregators and ecosystem intermediaries) in relation to user-permissioned financial data sharing. In addition, my testimony is intended to inform the Task Force about the progress and maturity of FDX since its launch less than three years ago, including a detailed view of FDX's mission, structure, and vision to implement common, interoperable, and royalty-free technical standards for user-permissioned financial data sharing.

As a technical standards body, FDX is currently barred from taking positions on most legislative and regulatory policy issues. FDX does engage in "educational advocacy" to ensure that regulators, legislators, and policymakers are educated and fully aware of the work FDX is doing, the way this work interacts with certain policies and regulations, and the way innovations across the financial services ecosystem are giving consumers and businesses the ability to securely use and share their financial data.

¹ [FDX Members](#)

² From *FDX Taxonomy of Permissioned Data Sharing v. 1.1*: **Data Providers**: the entities who hold End Users' Financial Account Information, including, without limitation to banks, credit unions and brokerages.

³ From *FDX Taxonomy of Permissioned Data Sharing v. 1.1*: **Data Recipients**: service companies, applications (financial apps), Fintechs, financial institutions, products and services where End Users (on their own or through their End User Delegates) manage or act on their finances, whether actively managing their finances (such as moving money or applying for credit) or passively doing so (such as garnering recommendations or insights).

⁴ From *FDX Taxonomy of Permissioned Data Sharing v. 1.1*: **Data Access Platforms**: intermediaries that facilitate financial data access, transit, storage and/or permissioning on behalf of Data Recipients or End Users, also commonly referred to as "data aggregators". In some cases, Data Access Platforms may not have a direct relationship with the End User. The data may be passed through without modification or may be normalized in line with permitted objectives (e.g., parsed for readability or used to confirm other data). Data Access Platforms should not be misidentified with parties who do not obtain End Users' consent but gather data, sometimes referred to as Data Brokers⁵ or Data Harvesters.

FDX also advocates for technical specifications and standards designed and implemented by the financial services industry for user-permissioned data sharing as opposed to regulatory or government mandated technical standards.

Ultimately, FDX believes open banking or open finance has two halves – a “What” and a “How.” The “what” is often determined by legal agreements between financial services entities or defined in legislation or regulation. The “what” encompasses many of the decisions and guidance about financial data rights, determinations about what constitutes derived data and the way different entities and roles within data sharing are regulated.

On the other hand, the “how” of open banking or open finance involves the technical means and methods that enable the full scope of user-permissioned financial data to be securely shared and transmitted between data providers, data access platforms and data recipients. This “how” is where FDX is succeeding in defining a common, interoperable and royalty-free API standard and accompanying guidance so that financial data sharing is consumer-centric, complete, secure and uniform regardless of where a user banks, what financial services they access or what fintech apps they may choose to use.

Considering this, and in the context of the ever-changing roles and relationships between different financial services entities involved in financial data sharing, FDX believes it is important to provide the task force with a perspective on how user-permissioned financial data sharing is actually working in the market today.

Historical Snapshot of Standardization of User-Permissioned Data Sharing

Over the last two decades, significant innovation in financial services has been driven by end user demand for online financial management services, payments, credit decisioning and more that requires access to and sharing of financial data. While these new financial technology tools are often provided by companies that are not affiliated with an end user’s primary financial institution, financial institutions themselves also offer financial technology products and services to their customers and are increasingly on the receiving end of financial data from other financial institutions as directed by their customers.

To utilize these services, users need the ability to be authenticated so they can authorize access to their financial data from their financial institutions to other financial data parties in a convenient, secure, and reliable manner.

In order to give these parties access to their financial records, end users have historically provided their login credentials to financial applications or data access platforms (known as credential-based access). In most cases, financial apps do not store a user’s login credentials, but instead pass these credentials via an Application Programming Interface (API) to the data access platform. The financial application or data access platform can then access the financial institution website and retrieve the users’ data (this process is known as screen scraping).

While credential-based access and screen scraping have provided a pathway for consumers to use and share their own financial data to date, this legacy technology is inefficient and places stress on financial institutions due to the number of automated logins. Finally, and most importantly, this method of

consumer authentication and data access requires the sharing of sensitive consumer login credentials and provides limited consumer control over the amount of data consumers share with third parties.

Fortunately, market adoption of a more efficient and secure method of data sharing began a few years ago and should eventually replace shared login credentials and screen scraping in most scenarios. Specifically, tokenized access, in concert with API-based data collection, allows a user to be securely authenticated by their own financial institution and authorize the data provider to supply only the data they want to share. In fact, APIs make user-permissioned data sharing easier, more accurate and more secure. Not only do they remove credential sharing and provide dedicated data access, but APIs provide the ability for data providers to give consumers control over the type of data that is shared, with whom, for how long and for what purpose.

While the advent of APIs for financial data sharing has begun to change the user-permissioned data landscape, there was still a missing element – standardization. In fact, without standard APIs and additional standardization of authentication, authorization, certification, user experience and consent guidelines, financial institutions, financial data access providers and fintech applications and services will remain fragmented – using incompatible APIs, different data scopes, processes and even definitions for how a user is able to permission use of their own financial data.

Accordingly, FDX was born out of a desire among all entities in the user-permissioned financial data ecosystem to have standardized APIs available that can replace the need for screen scraping for the same user-permissioned financial data elements.

Key Points for the Task Force:

In an effort to provide the task force with thoughts on issues as requested in testimony for this hearing, I would like to list a few key points that I believe are critical for the task force to understand and consider related to the current state of consumer data sharing, industry standardization and the benefits that permissioned financial data sharing is delivering to consumers and small businesses.

Five 5 Principles of Consumer Data Sharing

The ability for consumers to access and share the entirety of their own financial data, whether via authorized or direct access, is the central pillar upon which FDX is built. And FDX believes accessible, user-permissioned financial data sharing inherently gives consumers control of their data. Such an approach empowers End Users to better understand, leverage, and benefit from their own financial data and improve their financial lives. A consumer-centric approach also facilitates greater consumer protection and full access to financial data that can improve financial literacy, financial decisions, and financial convenience.

In order to deliver a system of financial data sharing that provides these consumer benefits, FDX believes five core principles must be present to ensure that all participants in the user-permissioned data sharing ecosystem serve the needs of consumers. These are:

- 1.) **Control** - Consumers should be able to permission their financial data for services or applications.

- 2.) **Access** – End Users should have access to their data and the ability to determine which entities will have access to their data.
- 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.
- 4.) **Traceability** - All data transfers should be traceable. Consumers should have a complete view of all entities within the user-permissioned financial data ecosystem that are involved in the data sharing flow.
- 5.) **Security** - Financial data parties should follow industry best cybersecurity practices across the whole of their organization for safety and privacy of data during access and transport and when that data is at rest.

Benefit of user-permissioned data sharing:

Before anyone coined the term open banking or open finance, consumer demand for budgeting, payments, digital lending, importing tax data and other fintech applications served as a catalyst for the innovative and diverse financial services marketplace we have in the U.S. today. And consumers are the beneficiaries of this competition and innovation because they now have more choices, great efficiency and lower costs for financial services. Some specific benefits of consumer permissioned financial data sharing include:

- 1.) **Enhanced transparency into one's financial circumstances** - Put simply, the ability to access and share the full extent of a consumer's financial data now allows consumers to actually see their money, debt, investments and bills all in one place which allows for better management and more informed financial decision making.
- 2.) **Expansion of credit access and lower cost of credit** - Financial data sharing is accomplishing a long-held goal of this Committee by broadening credit access to thin-file or no-file borrowers because lenders are able to determine credit worthiness from cash flow data when a traditional credit score is limited or incomplete.
- 3.) **Increased financial literacy and utilization of financial data** – Financial data sharing is giving consumers the same powerful tool that many companies have utilized for years – Big Data. And while the notion of big data often has a negative connotation, when a consumer has the reins of all of their own data, they are able to better understand their own financial lives and use it to leverage better financial outcomes.
- 4.) **Lower Costs** – The provision of digital and automated financial services tools help consumers manage their money, including by avoiding overdraft fees and lowering lending costs due to more efficient processes, a better determination of credit worthiness, better rates and lower fee products.

Distinction of User-Permissioned Financial Data Sharing vs Data Collection & Data Harvesting

It is important for the task force and regulators to consider a bright line distinction between user-permissioned financial data sharing, and activity undertaken by actors like data brokers or data

harvesters. From an FDX standpoint, I want to stress to the Task Force that all financial data used and accessed through the FDX API standard must be user permissioned. In other words, no financial records will be accessed without a consumer's full permission and control. This contrasts sharply with practices where data about consumers is collected and/or sold without express consumer consent, consumer control or consumer awareness. This distinction is important as the Task Force and Committee consider privacy questions about financial services activities involving consumer financial data.

Technical Standards Best Left to Industry

FDX firmly believes that market-led standards are best suited to define the technical aspects of user-permissioned data sharing in the US market. FDX believes it would be a mistake for Congress or the CFPB to attempt to define technical standards in any way.

Common, interoperable, royalty-free, and market-led technical standards not only maintain accessibility and innovation in the financial services industry but propel them forward. Specifically, common market-led standards level the playing field and lower the barriers to entry for market entities of all shapes and sizes because the cost and efficiency of connecting to implementations of the same standard across the ecosystem is much lower than a multitude of proprietary standards.

Open market-led standards are also able to be continually adapted with balanced input from all market participants. And by their very nature, market-led technical standards adapt to the needs of the market. Whether it is a new product and service that technical standards need to address or new technologies that should be implemented, market-led technical standards are never wed to one approach, one technology or one market segment. They grow, mature, and change with the market and with consumer demand.

In addition, FDX technical standards can be tailored to accommodate any regulatory or legal requirements in a given jurisdiction. As mentioned, FDX is neutral on policy issues and seeks to implement technical standards to accomplish the "means and methods" of user-permissioned data sharing in a way that is responsive to market needs as well as any legal or regulatory compliance requirements. FDX will ensure its standards meet any principles or requirements that Congress or the CFPB may place on user-permissioned data access.

FDX also wishes to make the Task Force aware of the way FDX standards refer to and build upon the work of other existing global standards organizations like the Internet Engineering Task Force (IETF), the Open ID Foundation (OpenID), National Institute of Standards and Technology (NIST) and the FIDO Alliance (FIDO). In other words, FDX does not seek to "reinvent the wheel" where existing open standards exist and instead seeks to provide technical standards that provide foundational global interoperability for a financial services industry that is increasingly borderless and regulatory structures that vary between jurisdictions. Indeed, technical harmonization around the globe, especially on privacy, security, and authentication, is critically important and FDX is actively engaged with and following other global open banking and open finance regimes around the world.

But don't just take my word for it. I encourage the Task Force to consider the experience of other market-led approaches to financial technology innovation like online banking, mobile banking, and the EMV (EuroPay, Mastercard, Visa) chip replacing the magnetic stripe on cards. All of these significant

technological transitions in financial services moved forward without government mandates or artificial timelines. Further, outside the fintech sector – examples like Bluetooth, Fast Identity Online (FIDO), Universal Serial Bus (USB) and the Payment Card Industry Data Security Standard (PCI DSS) show how market-driven solutions have been successful.

Alternatively, regulatory-led or government mandated technical standards related to financial data sharing and open banking have proven to be limited in scope, time consuming and unable to adapt quickly to market conditions and technological changes. Also, government mandated technical standards have the potential to significantly slow or freeze innovations because technical standards become a compliance exercise rather than an attempt to define standards that are responsive to market needs and consumer demand.

It is also important to consider the market dynamics of jurisdictions pursuing regulated or government mandated standards. Often these markets have a single financial regulator and a concentrated banking market (i.e., 9 major banks in the UK, 4 in Australia, 4 in Mexico, etc.). The resulting technical standards often apply to a significant portion of the market all at once. However, without an ecosystem approach that considers the needs of a large and complex market, multiple financial regulators and its diverse participants (especially important in the US with over 14,000 financial institutions), such technical standards can be ill-fitting to smaller market participants.

Shifting Roles within Consumer Permissioned Data Sharing

FDX defines four key roles within user-permissioned data sharing, End Users, Data Providers, Data Access Platforms and Data Recipients.

- **End Users:** include consumers, individuals acting in a business capacity, and entities, such as a business or other legal entity, who are giving permission to share their data.
- **Data Providers:** the entities who hold End Users' Financial Account Information, including, without limitation to banks, credit unions and brokerages.
- **Data Recipients:** service companies, applications (financial apps), fintechs, financial institutions, products and services where End Users (on their own or through their End User Delegates) manage or act on their finances, whether actively managing their finances (such as moving money or applying for credit) or passively doing so (such as garnering recommendations or insights).
- **Data Access Platforms:** intermediaries that facilitate financial data access, transit, storage and/or permissioning on behalf of Data Recipients or End Users, also commonly referred to as "data aggregators". In some cases, Data Access Platforms may not have a direct relationship with the End User. The data may be passed through without modification or may be normalized in line with permitted objectives (e.g., parsed for readability or used to confirm other data). Data Access Platforms should not be misidentified with parties who do not obtain End Users' consent but gather data, sometimes referred to as Data Brokers or Data Harvesters.

While each of these roles have traditionally been played by specific market actors (financial institutions have played the role of data providers, data aggregators and other intermediaries have played the role of data access platforms and fintechs have played the role of data recipients), today's user-permissioned

data ecosystem involves financial services firms often playing many of these roles, and sometimes simultaneously. For example:

- Financial institutions increasingly play the role as both data providers and data recipients when their customers seek access to account data from other financial institutions or seek credit that may involve cross-institution data sharing.
- The role of a data access platform has expanded to include different industry utilities, intermediaries and approaches. In addition, some data aggregators are serving functions for financial institutions to allow for more seamless data sharing experiences, like managing end-user permissions and obtaining consent.
- While still in its infancy, even fintech apps may soon move beyond the role of data recipients and into the role of data providers with two-way data sharing or reciprocity that provides a flow of fintech data back to financial institutions.

With this in mind, FDX standards are focused on the role itself rather than the type of entity performing said role and FDX encourages future Task Force considerations around consumer data sharing to also consider the role in the ecosystem versus the type of entity playing it.

Views on CFPB Rulemaking

FDX submitted comments⁵ to the Consumer Financial Protection Bureau's (CFPB) Advanced Notice of Proposed Rulemaking (ANPR) requesting information related to consumer access to financial records and the development of regulations to implement Section 1033 of the Dodd-Frank Act. In addition, FDX was mentioned or referenced in relation to how the financial industry is creating technical standards in almost half of the comments the CFPB received on the ANPR.

While FDX is unable to comment on specific elements of potential CFPB rulemaking, or even if CFPB should proceed with rulemaking at all, I would like to submit the following contextual thoughts:

- FDX believes that the ability for consumers to access, control and share all of their own financial data, whether via authorized or direct access, in a transparent, traceable and secure manner is paramount.
- FDX believes that consumers expect full access to their own data to use, share and leverage to their financial benefit. We believe that consumers also expect that they alone should have control of how their data is permissioned, shared, used, or accessed, as well as having the ability to revoke such choices. We believe that consumers expect to be clearly informed about who has access to their data, what purpose it will be used for and for how long it will be used. Finally, we believe consumers fully expect that their data will be transferred as needed in a secure manner, and that if there is an issue that results in loss, that they will be made whole.
- FDX believes that when a system of financial data sharing appropriately provides FDX's Five Principles (Control, Access, Transparency, Traceability and Security), consumers benefit in the

⁵ <https://www.regulations.gov/comment/CFPB-2020-0034-0019>

form of cost savings, transparency, efficiency, control, enhanced financial awareness and security.

- FDX believes that a non-profit and market-led technical standards body is best positioned to unify the financial industry around common, interoperable, royalty-free technical standards for user-permissioned data sharing. Such market-led standards, such as the FDX API, can be tailored to accommodate regulatory requirements and enable the most secure and transparent consumer data access possible while preserving the ability for the market to continue to innovate and utilize the best technological approaches for data sharing.
- FDX believes that the CFPB and other regulators can and should do more to prioritize the adoption of common and interoperable APIs and reduce structural disincentives that might delay adoption and implementation of APIs. This includes formal reference or acknowledgement of market-led standards to show approval of the standards themselves and the direction of the work. This is especially important for smaller entities. Such support also includes better training and understanding from the top of the agencies down to those involved in examination and regulatory enforcement so that all are aware of how standards are being implemented and used in the marketplace.
- FDX believes that regulatory modernization must prioritize harmonization. FDX encourages regulators to work together where possible so that industry standards are not caught between competing, overlapping or disjointed requirements.
- FDX believes that public policy around consumer data sharing must balance the need for consumers to be able to access and share the full extent of their own financial data with data recipients who may have no relationship with the data provider with data providers, like banking organizations, to maintain sound risk management practices, conduct activities in a safe and sound manner, and remain consistent with applicable laws and regulations.
- FDX believes that rapid innovation in the marketplace and evolving and overlapping industry roles within the user-permissioned data sharing ecosystem means that policy must consider addressing the role that is being played rather than focusing on a specific market segment or entity playing the role.

Conclusion:

As the Director of Public Affairs for the Financial Data Exchange, I am thankful for the opportunity to provide testimony to the Task Force today. I believe it is important for Task Force Members to be aware of the policy issues inherent to user-permissioned financial data sharing, but also the immense progress that the industry has made in regard to technical standards which enable this data sharing, and which are powering the transition from screen scraping to interoperable APIs. I welcome your questions.

Appendices

- A. Structure & Details of the Financial Data Exchange
- B. FDX Five Principles of Consumer Data Sharing
- C. Publicly Announced Data Sharing Agreements Mentioning FDX API

Appendix A: Structure & Details of the Financial Data Exchange

In less than three years, FDX not only has significant momentum with over 200 members and over 22 million consumers converted from screen scraping to the FDX API, but it is also best positioned to continue unifying the financial industry around its common, interoperable, and royalty-free technical standards. FDX can make this claim because it has the broad commitment, investment and participation of its members from across the financial data ecosystem, including financial institutions, financial data aggregators, fintechs, payment networks, consumer groups, financial industry groups, industry utilities, service providers, other permissioned parties and even individual academics and experts in the field.

As a technical standards body, FDX's members develop, enhance and adapt the FDX API and accompanying standards via a board of directors and over 30 different committees, working groups and task forces. FDX maintains fairness by ensuring that its membership is diverse and that all market segments within the larger ecosystem have the opportunity to participate in the work. FDX also employs a balanced leadership approach across all work streams with each committee, working group and task force co-chaired by a financial institution and a non-financial institution. Finally, every FDX member organization, regardless of size, type, or dues, has a single and equal vote.

FDX abides by the mantra of "Best idea wins," irrespective of firm size or type. The FDX board voting structure is also balanced by giving different market segments equivalent voting representation by requiring a super-majority of board members across industry sectors to agree on major decisions. The FDX API specification itself is free for any organization to download and use and membership starts with a no-cost tier for non-profit consumer advocacy groups and an affordable and revenue-based structure for all other entities.

Simply put, FDX's goal is to develop, promote and seek broad adoption of neutral market-led technical standards that enable the most secure and transparent consumer data access possible while preserving the ability for the market to continue to innovate and utilize the best technological approaches for data sharing.

Below is a list of FDX's Committees Working Groups and Task Forces

Committees

Audit & Finance	Assists the Board in discharging its responsibilities relating to independent oversight, financial reporting, budget, internal controls and procedures and related matters. It performs both an audit and a finance role.
Compensation	Determines FDX's overall compensation structure, policies and programs, as well as oversees compensation of FDX's Managing Director, other executives and key employees.
Executive Steering (ESC)	The ESC is comprised of nine sustaining members, with a similar industry representation to the Board, that has the authority of the Board (subject to certain restrictions and override authority of the Board) and meets monthly. The FDX Board has ultimate authority with respect to any decisions of the ESC.

Marketing, PR & Government Affairs	Shares FDX stories and milestones, and seeks to increase membership in FDX by raising awareness of the benefits of FDX's common interoperable standard.
Technical Review (TRC)	Provides technical oversight to all working groups, including technical standards, versioning, and related matters. The TRC's role involves oversight and alignment of artifacts produced by technical working groups.

Working Groups

API & Data Structures	Maintains, revises, and releases the API and data specification. In addition, provides any necessary artifacts in support thereof, such as meta data, dictionaries and use cases.
Canada	Assesses the potential for use of the FDX API in Canada, recommends any changes to the FDX API that may be required for use in Canada, and if suitable, advocate the use of the FDX API in Canada.
Consumer Advocacy Group Advisory Board	Composed of Consumer Advocacy Groups, this group provides advisory services to the FDX Board and Working Groups on a mutually agreed upon basis.
Global Summit	Oversees the planning and execution of all FDX biannual Global Summits. Determines the topics, speakers, presenters, schedules, formats, and appropriate venues for each summit.
Marketing & Public Relations	Addresses all topics related to Marketing and Public Relations matters. This includes raising awareness of the benefits of FDX standards and other goals of the Marketing, PR & Govt Affairs Committee.
OFX	Provides on-going support and enhancements as needed to the OFX specification and associated services, in a secure and user-controlled manner.
Qualification & Certification	Develops and maintains the FDX product certification program, Foundational Certification, to ensure technical interoperability among FDX member organizations. Further, it oversees the development of an FDX Directory and Registry.
Security & Authentication	Develops and maintains the FDX API Security Model and standards, and related artifacts in support thereof.
U.S. Government Affairs	Amplifies the efforts of the Marketing & Government Affairs Committee in its educational and outreach efforts with governmental bodies (regulatory, appointed and elected).
User Experience	Develops industry guidelines and best practices for the user experience when sharing and accessing their financial data. The overall goal is a consistent user interface across the industry driven by FDX's core principles.

Standing Task Forces

API Governance & Authoring	Task force to oversee documentation authoring process so RFC author proposals are formulated in line with the authoring strategy.
Canadian Government and Regulatory Engagement	Task force to guide the educational engagement of FDX and its members with government representatives, policymakers, regulators, and industry stakeholders in Canada.
Canadian Technical	Task force to oversee all technical work for Canada, to align FDX technical specifications for application in the Canadian market, and to make recommendations to other FDX working groups.
Consent API	Task force to develop supporting Consent API to synchronize the consent experience and enable transmission and presentation of consistent data sharing consent between entities in the ecosystem.
Consent Management & Consent Dashboard	Task force to author User Experience for consent management, consent parameters and consent revocation in consent dashboards.
Governance and Oversight	Task force to oversee overlapping task force issues within User Experience and help the working group determine prioritization.
Money Movement Planning	Task to incorporate money movement and payment capabilities into the FDX API including features, user experience, security, interoperability and certification.
Sensitive Data Solutions	Task force to develop a solution for use cases requiring use of sensitive data that satisfies the use case while maintaining security and privacy.
Strategic Planning	Task force to develop the strategy, annual plan and priorities for all FDX activities and working groups that will deliver on the FDX mission.
Tax Forms	Task force to develop FDX formatted tax forms and schemas and transition providers away from using legacy tax data formats.
Taxonomy	Task force to author and publish updates to FDX Taxonomy for use within FDX and to inform external stakeholders.
Use Case Development & Maintenance	Task force to explore and develop user-permissioned data sharing use cases.
User Journeys	Task force to author consent flow and use case journeys for evolving the User Experience Guidelines.
User Experience Research	Task force to evaluate needs, execute and report out on user experience research.

Special Purpose Task Forces

App Registration	Task force of the Security & Authentication working group to explore scalability issues related to Recipient Application Registration between Data Access Platforms and Providers and to explore standards for Provider Automated Application Registrations.
------------------	--

Cryptocurrency	Task force of the API working group to develop attributes and modifications allowing FDX use for cryptocurrency portfolios, transactions, exchanges and tax reporting.
Fraud Monitoring	Task force of the API working group to build fraud monitoring and controls into the FDX specification including modeling use case-based fraud scenarios, data required for suspicious activity and fraud reporting.
Data Clusters	Task force of the User Experience working group to determine data cluster grouping, consumer understanding, visual treatment and mapping to use cases. The task force will also define consent object, enabling consent grant management and requirements for consent API technology.
Certification Model	Task force of the Qualifications & Certification working group to develop FDX's Certification model 1.0.
Directory	Task force of the Qualifications & Certification working group to create and maintain an FDX Registry of membership, technical conformance and relevant parties.
Notifications	Task force of the API working group to define the notification framework and specify security guidelines, specifications, document use cases and operation best practices for event notification.
Testing & Tooling	Task force of the Qualifications & Certification working group to develop test suites for FDX certification.
Intermediary Identity	Task force of the Security working group to specify modifications and methods to use the OAuth framework so that Data Access Platforms are able to perform functions for Data Recipients like end-user transparency, registration and traceability functions.
FAPI & FDX API Security Profile Harmonization	Task force of the Security and Authentication working group to identify elements of FAPI specification for FDX to deem normative and to establish reference to FAPI certification as a requirement for FDX certification.
Recipient Certification Requirements	Task force of the Qualifications & Certification working group to determine expectations and responsibilities of data recipients and what must be provided for certification.

FDX Deliverables to the Marketplace

Since its launch in 2018, FDX has delivered key standards, guidelines, and best practices into the marketplace. Here are a few of the key FDX deliverables to date and those anticipated in the near future:

- 1.) FDX API Specification: Currently at version 4.6 (with FDX API 5.0 anticipated release before the end of October 2021), the FDX API is the foundation of FDX data sharing standardization and offers consumers the ability to access over 620 different financial data elements, including banking, tax, insurance, and investment data, making it one of the most comprehensive Open Finance standards in the world. The FDX API is designed to enhance interoperability and

performance for the full range of both currently defined use cases as well as those anticipated in the future. The FDX API utilizes foundational and globally interoperable standards for security, authentication, data transfer, authorization, API architecture, and identity and represents a global best-in-class solution set for user-permissioned data sharing that limits the risk of data inaccuracy.

- 2.) User Experience & Consent Guidelines: As adoption and implementation of the FDX API expands, these guidelines are the product of months of work and significant consumer testing and are intended to accelerate design decision-making during implementation of data sharing experiences. The User Experience & Consent Guidelines also seek to align user-permissioned financial data sharing with consumer understanding, preferences, and expectations. These guidelines specify what information and control must be given to end users to ensure consistent data sharing experience regardless of where their data is held or who they are seeking to share it with. Specifically, concepts such as financial data sharing, data flow, and data clusters, followed by specific user experience guidelines for an end user grant consent journey for financial data sharing are defined in this documentation. Eventually, FDX certification will involve compliance with User Experience requirements and the guidelines will be tailored to each FDX defined Use Case.
- 3.) Taxonomy of Permissioned Data Sharing: In an effort to align industry stakeholders and help regulators and policymakers better understand and define the various roles and perspectives within the user-permissioned financial data ecosystem, FDX maintains a set of common terminology to be used as a taxonomy for the ecosystem. This documentation also includes a conceptual flow model to show how End Users interact with different participants within the current ecosystem that is evolving from legacy to new technology. The Taxonomy document⁶ also provides a cursory comparison of similar terminology in the permissioned data sharing space among other parties such as the US Department of Treasury, US Consumer Financial Protection Bureau, and other key parties in the financial services industry.
- 4.) Global Registry: FDX is currently building an authoritative registry of trusted entities to help the user-permissioned financial data marketplace clearly identify ever evolving technologies and new market entrants, as well as the web of often proprietary, incomplete, and incompatible technical standards that complicate the market today. The FDX Global Registry will enable those entities operating within the FDX and other ecosystems to reliably identify and verify trusted organizations and acts as a market incentive to all entities to ensure the accuracy of the data itself, as well as the transfer or exchange of that data. This registry will also support interoperability across a variety of financial services, industry sectors and jurisdictions. In addition, the FDX registry will provide information regarding reliability and repeatability of the performance of data, traceability, transparency, and trust in FDX Certification(s), accelerates the adoption of standards, and serves to bind the ecosystem players to each other. FDX intends the

⁶ FDX Taxonomy of Permissioned Data Sharing v. 1.1 listed as Appendix C

Global Registry to act as a non-profit, non-commercial, technology agnostic, multi-tenant, cross-sector, authoritative international resource as well as a center of technical excellence.

- 5.) Certification Use Cases: FDX use cases are testable data profiles that measure functional capability of an API against a broad business use of financial data. FDX defines these data profiles as a means of establishing functional baselines that APIs must meet to be considered useful by data consumers, but FDX use cases do not limit consumer data access. In fact, FDX encourages sharing of other data even when not defined in use cases as necessary to meet innovation and business goals. FDX recommends that any such sharing be in line with FDX's five principles of financial data sharing – Control, Access, Transparency, Traceability and Security (CATTS). So far, FDX has approved Personal Financial Management (PFM) and Credit Management and Servicing (to support credit decisioning and scoring) use cases. It expects to define and certify specific use cases in the future, such as money movement, account verification, tax preparation and fraud reporting.
- 6.) Developing a Certification Program: Creating a standard alone cannot promote, drive adoption, or guarantee adherence to the standard. A qualification and certification program are needed to ensure common implementation and interoperability of any technical standard and further limits the risk of data inaccuracy. Products (i.e., programs, services, and apps for consumer permissioned financial data sharing) can be approved by a certification program to test the technical compatibility/interoperability, prior to being marketed as a compliant product, or getting access to certain intellectual property rights. Work continues on FDX's certification platform, and FDX recently released foundational requirements covering availability, performance, and security that implementations of the specification must meet to apply for a FDX use case certification.
- 7.) Annual Strategic Survey: FDX's annual strategy survey gives FDX members the ability to be heard and direct the organization's work towards the highest priority issues in the marketplace. These surveys ensure that industry standards work remains agile and adaptive. FDX may also soon explore surveys that allow non-FDX members to weigh in on issues that need attention and standardization to ensure that FDX is responsive to all market issues in the user-permissioned data ecosystem.

Appendix B: FDX Five Principles of Consumer Data Sharing

FDX believes accessible, user-permissioned financial data sharing inherently gives consumers control of their data. Such an approach empowers End Users to better understand, leverage, and benefit from their own financial data and improve their financial lives. A consumer-centric approach also facilitates access to financial data that can improve financial literacy, financial decisions, and financial convenience.

In order to deliver a system of financial data sharing that provides these consumer benefits, FDX believes five core principles must be present to ensure that all participants in the user-permissioned data sharing ecosystem serve the needs of consumers. These are:

- 1.) **Control** - Consumers should be able to permission their financial data for services or applications.
 - All entities within the user-permissioned financial data ecosystem should provide clear, intuitive navigation and information to consumers, allowing informed decision making on sharing financial data.
 - 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** – End Users should have access to their data and the ability to determine which entities will have access to their data.
 - Intuitive navigation: The authentication process should avoid unnecessary steps or language that delays, interrupts, or impedes access.
 - 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.
 - Responsible Access: Consumers should provide informed consent (with the ability to revoke that consent) for any and all access granted to entities within the user-permissioned financial data ecosystem. These entities 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.
 - Consumers should be able to view who they have permissioned, as outlined above in “Control.”
 - 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 entities within the user-permissioned financial data ecosystem that are involved in the data sharing flow.
 - 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 data

provider through the financial data access platform and to the financial data recipient) in order to aid the pinpointing of potential errors or suspicious connections.

- 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 should follow industry best cybersecurity practices across the whole of their organization for safety and privacy of data during access and transport and when that data is at rest.
- All entities within the user-permissioned financial data ecosystem need to provide clear definitions on data usage and privacy, permitting consumers to make educated decisions.
 - All entities 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.
 - 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.



**Appendix C: Examples of Publicly Announced Data Sharing Agreements
Featuring the FDX API**

- [TD Bank joins the Akoya Data Access Network to accelerate Open Finance](#) – Sept 13, 2021
- [Pentadata Announces Open Finance Integration with Akoya](#) – July 29, 2021
- [Wells Fargo joins the Akoya Data Access Network to advance API-based financial data aggregation](#) – June 22, 2021
- [Capital One and Plaid Announce New Data Sharing Agreement](#) – June 8, 2021
- [Jack Henry and Akoya Offer 4.8 Million Financial Institution Customers API-Based Access to Their Financial Data](#) - May 10, 2021
- [Jack Henry-Finicity partner to empower community financial institutions with open banking capabilities](#) - May 5, 2021
- [Akoya adds JPMorgan Chase to its Data Access Network](#) – February 17, 2021
- [Finicity Announces Secure Data Access Agreement with Brex](#) - December 18, 2020
- [Akoya and U.S. Bank team up to accelerate safe, secure, and transparent consumer-permissioned financial data access](#) - November 16, 2020
- [Finicity and BMO Harris Bank Finalize Secure Data Access Agreement](#) - November 12, 2020
- [Wells Fargo and Envestnet | Yodlee Sign Data Exchange Agreement](#) - September 24, 2020
- [FINICITY FINALIZES SECURE DIRECT DATA AGREEMENT WITH CHARLES SCHWAB](#) - September 18, 2020
- [TD enters into North American data-access agreement with Finicity](#) – August 7, 2020
- [TD enters into North American data-access agreement with Intuit](#) – September 2, 2020
- [Financial Institutions Can Empower Consumers to Securely Share Their Data with New Aggregation Solution from Fiserv](#) - September 3, 2020
- [U.S. Bank and Fiserv sign agreement to simplify data exchange between customers and applications](#) – March 9, 2020
- [Envestnet | Yodlee and JPMorgan Chase Sign Data Agreement to Enhance Consumer Data Protections, Bolster Overall Data Connectivity and Reliability](#) – December 5, 2019
- [U.S. Bank signs agreements with top data aggregators and fintechs, bolstering API efforts](#) – September 23, 2019
- [Wells Fargo and Plaid Sign Data Exchange Agreement](#) – September 19, 2019
- [Envestnet | Yodlee and Charles Schwab Enter Financial Data Access Agreement](#) – April 16, 2020
- [Charles Schwab Reinforces Its Commitment to Customer Data Protection](#) – April 16, 2020
- [Wells Fargo Surpasses One Billion API Calls](#) – February 11, 2020
- [JPMorgan Chase, Envestnet | Yodlee Sign Agreement to Increase Customers' Control of Their Data](#) – December 5, 2019
- [Plaid Signs Data Agreement with JPMorgan Chase](#) – October 22, 2018

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

Regarding

“Preserving the Right of Consumers to Access Personal Financial Data”

September 21, 2021

Raúl Carrillo, Esq.
Associate Research Scholar, Yale Law School
Deputy Director, Law and Political Economy Project

Background & Summary	2
Dodd-Frank & Data Governance	6
Consumer Financial Protection: From Market Power to Platform Power	7
Data Security	8
Data Privacy	9
Fair Competition	10
CFPB Recommendations	11
CFPB Section 1033 Rulemaking Should Promote Consumer Control in the Context of Data Minimization	11
FCRA Rulemaking Should Cement the Bureau’s Authority over Data Aggregators	12
CFPB Rulemaking Should Grant the Bureau Authority to Supervise Data Aggregators	12
CFPB UDAAP Enforcement Should Center Unfair Data Collection	13
Congressional Recommendations	15
Congress Should Structurally Separate Commercial and Financial Power	15
Congress Should Constrain Data Usage to a Short List of Permissible Purposes	15
Financial Inclusion in the Informational Economy	18

Background & Summary

Chair Lynch, Ranking Member Davidson, distinguished Members of the Task Force, thank you for inviting me to testify. I offer my testimony as an Associate Research Scholar at Yale Law School. I am also the Deputy Director of the Law and Political Economy Project.¹ I have previously worked as an attorney for low-income consumers and served as Special Counsel to the Enforcement Director of the Consumer Financial Protection Bureau (CFPB).

My previous remarks before this task force have called for policymakers to consider the deeper impacts of nascent financial technologies on our society and principles of democracy. Today, I repeat the call for policymakers to adopt a bright-line, precautionary approach to technological developments involving financial products, sectors, and systems.² What industry calls "innovation" is often easily mapped to a longstanding financial service and therefore the substance of existing laws should govern.

However, in the cases when innovation is not easily mappable, it is often due to adoption of the tech company business model: mass data collection. Deeper changes in the information economy must inform regulatory responses. It is understandable to want regulations that endure the test of time. However, it is impossible to be truly "technology-neutral", as industry desires, because neither laws nor technologies are neutral. They are designed to serve some interests over others.

This morning, I have the luxury of presenting alongside Chi Chi Wu of the National Consumer Law Center (NCLC) and will defer to the NCLC on many urgent questions of consumer protection. Broadly, I agree that consumers deserve more control over their data relative to banks and other financial institutions. That said, consumer rights to access, review, manage, correct, and delete data about themselves can only be meaningful within a broader policy that minimizes data collection and inappropriate usage in the first place. Consumer control over financial data must operate within a broader paradigm of *data minimization*: collecting and processing only the minimum amount of data required to carry out an explicit, narrow purpose.³

Currently, every online interaction leaves "digital breadcrumbs" (purchasing histories, visited websites, and IP addresses, etc.) even if data collectors have not yet identified a purpose for the collection.⁴ A mostly unregulated data broker industry adds payments and credit data to

¹ "The Law and Political Economy (LPE) Project brings together a network of scholars, practitioners, and students working to develop innovative intellectual, pedagogical, and political interventions to advance the study of political economy and law." <https://lpeproject.org/>.

² See, e.g. Saule T. Omarova, *Dealing with Disruption: Emerging Approaches to Fintech Regulation*, 61 WASH. U. J.L. & POL'Y 27, 34-36 (2020) (discussing the problem with "smart" regulation: regulation that is "iterative, flexible, carefully tailored, risk-sensitive, and innovation-friendly."); JULIE E. COHEN, *BETWEEN TRUTH AND POWER: THE LEGAL CONSTRUCTIONS OF INFORMATIONAL CAPITALISM* 174, 182-187 (2019) (underscoring the importance of understanding platform digital activities in order to meet systemic threats).

³ Data minimization means that only those data are processed (collected, stored, mined, inferred, used for training algorithms) that are necessary. Mireille Hildebrandt, *Primitives of Legal Protection in the Era of Data-Driven Platforms*, 2 Geo. L. Tech. Rev. 252, 267 (2018).

⁴ Evan I. Schwartz, *Finding Our Way with Digital Bread Crumbs*, MIT TECH. REV. (Aug. 18, 2010), <https://www.technologyreview.com/s/420277/finding-our-way-with-digital-bread-crumbs/> [<https://perma.cc/M4SY-VJ9Z>].

data stocks regarding employment, marital status, homeownership status, medical conditions, and even our interests and hobbies, especially as articulated via social media. From the perspective of a human mind, there is too much data to process: the sets are too heterogeneous and the speed of analysis necessary to process them surpasses our abilities.⁵ But predictive analytics take massive amounts of surface data and infer latent data from them: powerful institutions try to forecast the future with precision, in real-time, and at scale. Mass financial surveillance eventually creates a detailed picture of our most private social, familial, romantic, religious, and political activities, offering a “picture of the person behind the payment.”⁶

Supporters of open banking are right that helpful data is underproduced and inequitably inaccessible to consumers given the centrality of reporting and scoring in our economy. Concern for consumer control also aligns with worries that big banks have monopolized data that could improve the profiles of consumers. Economists have argued for potential advantages to credit data sharing, including: increased competition in financial services markets; additional visibility, transparency, and completeness with respect to data dossiers; more efficient pricing of credit, debt management, and collection.⁷ The U.S. government also uses financial data for purposes of the administrative state and security state.

However, under the current regime, harmful data is also overproduced. The business models of most fintech companies ultimately rely on *data maximization*. Data maximization leads to harms that may not be obvious or even immediate. They are not evenly distributed across society. Some of these harms sound more readily in the law than others.

Most obviously, screen-scraping enables data aggregators to get more data than needed, including sensitive PII that can be hacked, stolen, sold, or overly shared. However, as a structural matter, there are two key differences between the products of yesterday and today: the volume of data extracted by each participant, and the multiplication of participants in the service chain.⁸ While a traditional credit card payment implicates a merchant, two banks and a payments processor, a payment made with a mobile wallet includes those parties and a mobile device maker, telecom or internet service provider, and often, but not always, a consumer-facing service provider that creates and manages the app that facilitates the payment. Each of the many entities involved in digital transactions may collect and share consumer data with other companies. While some data collection is necessary and appropriate, financial data collection tends to exceed this baseline. In many instances, financial service providers reserve broad rights to use consumer data for unrelated purposes. The roles of some of the parties involved are not always clear to consumers.⁹

⁵ See, e.g., Amy Kapczynski, *The Law of Informational Capitalism*, 129 YALE L.J. 1460, 1468 (2020).

⁶ Albert Fox Cahn & Melissa Giddings, *In the Age of COVID-19, the Credit Card Knows All*, SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT - URBAN JUSTICE CENTER (May 18, 2020), <https://www.stopspying.org/latest-news/2020/5/18/in-the-age-of-covid-19-the-credit-card-knows-all>.

⁷ Leon Yehuda Anidjar, Inbar Mizrahi-Borohovich, *Reinventing Credit Data Sharing Regulation*, 29 S. Cal. Interdisc. L.J. 177, 181–83 (2020).

⁸ Consumer Reports, Comments to the CFPB in Response to the ANPR Regarding Consumer Access to Financial Records Under Section 1033 of the Dodd-Frank Act, Feb. 4, 2021, <https://www.regulations.gov/comment/CFPB-2020-0034-0051>.

⁹ NCLC Written Statement for CFPB’s Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act, February 12, 2020, https://files.consumerfinance.gov/f/documents/cfpb_wu-statement_symposium-consumer-access-financial-records.pdf.

Financial data governance requires balancing the necessity of collecting highly personal and consequential information and the risk of harm that accompanies its processing. However, individual rights alone cannot account for the collective harms of datafication the flow within the financial system and beyond it. There are limits to the ways in which individual consumers can meaningfully make individual choices about how their personal data (or other people's data) can be used. The very point of data production in a digital economy is not to gain specific individual-level insights specific about specific data subjects. Rather, it is to put people into population-based relations with one another, and increasingly, to use a sample to make inferences about a class or population for the purpose of predicting behavior.¹⁰ People may volunteer payments and credit data that, when aggregated by corporations and governments, confers sensitive information about disadvantaged groups in unpredictable ways. Consent to all data use is not possible in this context.

Like NCLC and other public interest organizations, I believe the laws on the books grant regulators authority that should be vigorously exercised. Existing rules and laws were meant to substantively protect consumers at the time of their drafting, but may not have not been sufficiently updated to account for the ways in which technology has changed the relationships between consumers and the companies with which they engage.¹¹ New rules and laws must establish the rights of consumers to review and correct this information, and to ask companies to delete information, but within demarcated boundaries for the collection, processing, holding, and "sharing" of consumer financial data.

Ultimately, Congress must shift the burden of data protection from consumer, courts, and litigators, to regulators and technology companies. The collision of Big Tech and Wall Street in this space demands especially careful scrutiny: the fintech field is now being swarmed not by quick and nimble entrepreneurs but the largest tech and finance companies.¹² Companies, whether fintech, techfins, or any other permutation, should not be collecting any data that is not strictly necessary for the provision of a good or service. For example, signing up for a credit card online should not lead to targeted advertising (or new accounts). We should not be able to forfeit our rights to data privacy and security, in particular, simply by clicking "I agree", or providing token consent to data usage policies consumers do not understand and firms cannot and do not uphold.

This is especially important as we consider practices of "financial inclusion." Most fintech business models rely on data maximization that renders marginalized communities more vulnerable. In perhaps its most dangerous instantiation, many tech and fintech

¹⁰ For a general theory of data governance and democracy, informing this analysis, please see Salomé Viljoen, *Democratic Data: A Relational Theory for Data Governance* (Nov. 11, 2020), Yale L.J. forthcoming (unpublished manuscript) (manuscript at 3-9) (available at <https://ssrn.com/abstract=3727562>).

¹¹ See, e.g. Julie E. Cohen, *The Regulatory State in the Information Age*, 17 *Theoretical Inquiries L.* 369, 370 (2016) (arguing that the current regulatory institutions were designed in an era which industrialism was the principal mode of development and such institutions are not capable to deal with the challenges involved in the information age.)

¹² Zen Soo, *TechFin: Jack Ma Coins Term to Set Alipay's Goal to Give Emerging Markets Access to Capital*, South China Morning Post (Dec. 2, 2016, 9:38 PM), <http://www.scmp.com/tech/article/2051249/techfin-jack-ma-coinstermset-alipays-goal-give-emerging-markets-access>.

enterprises¹³ are attempting to create a biometric “decentralized and portable digital identity” to substitute for government ID or functionally become the government ID in some places.¹⁴ Many of these proposals involve biometric tools like facial recognition technology (FRT), iris-scanning, and palm prints, which are vehemently opposed by many privacy advocates.¹⁵

By law, this data is increasingly co-monitored by law enforcement via mass, pre-emptive, predictive, and perpetual surveillance. Poverty, family, criminal, immigration, and national security law have already made mass financial surveillance a channel for policing troubled by civil rights concerns. Moreover, the surveillance does not solve deeper issues of financial exclusion. The reasons people remain outside the financial mainstream in the United States are largely structural. Fintech applications are not solutions to structural problems.

As a general matter, the Bureau’s regulatory, supervisory, and enforcement authorities were established at a different time, with a different technological terrain. The fintech industry’s “endless capacity for self-referential growth”¹⁶ suggests prudence on behalf of policymakers. This testimony makes six concrete policy recommendations:

- 1) **Section 1033 Rulemaking Should Promote Consumer Control in the Context of Data Minimization**
- 2) **FCRA Rulemaking Should Cement the Bureau’s Authority over Data Aggregators**
- 3) **CFPB Rulemaking Should Grant the Bureau Authority to Supervise Data Aggregators**
- 4) **CFPB UDAAP Enforcement Should Center Unfair Data Collection**
- 5) **Congress Should Structurally Separate Commercial and Financial Power**
- 6) **Congress Should Constrain Data Usage to a Short List of Permissible Purposes**

¹³ Leon Periman & Nora Gurning, Focus Note: The Use of eKYC for Customer Identity and Verification and AML 8 (May 14, 2019), available at <https://ssrn.com/abstract=3370665> (last visited June 22, 2020).

¹⁴ See Ian Allison, *How Anti-Money-Laundering Rules Hinder Libra’s Mission to Reach the Unbanked*, COINDESK (Oct. 9, 2019), <https://www.coindesk.com/how-anti-money-laundering-rules-hinder-libras-mission-to-reach-the-unbanked/>; ET Bureau, *Aadhaar verdict: Telcos, banks & financial companies may feel the pinch*, THE ECON. TIMES (Sept. 27, 2018), <https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-verdict-telcos-banks-financial-companies-may-feel-the-pinch/articleshow/65973414.cms>.

¹⁵ Facial recognition software is likely to mislabel or misrecognize members of racial minority groups, especially Black Americans. See, e.g., Victoria Burton-Harris & Philip Mayor, *Wrongfully Arrested Because Face Recognition Can’t Tell Black People Apart*, ACLU (June 24, 2020), <https://www.aclu.org/news/privacy-technology/wrongfully-arrestedbecause>.

However, many civil rights advocates argue that the incompleteness of FRT databases is a good thing. Zoé Samudzi, “Bots Are Terrible at Recognizing Black Faces. Let’s Keep It that Way,” *Daily Beast*, February 8, 2019, <https://www.thedailybeast.com/bots-are-terrible-at-recognizing-black-faces-lets-keep-it-that-way>.

¹⁶ *Fintech: Examining Digitization, Data, and Technology: Hearing Before the U.S. S. Comm. on Banking, Hous., and Urban Affairs*, 115th Cong. 17 (2018) (Statement of Saule T. Omarova, Prof. of Law, Cornell L. Sch.), available at <https://www.banking.senate.gov/download/omarova-testimony-and-appendix-91818>.

Dodd-Frank & Data Governance

The main provision of Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank) in question today, Section 1033, has not yet been interpreted by the judicial system or any government agency.¹⁷

As we consider the scope of rulemaking under this provision, we should think of 1033 in the context of the CFPB's broader mission. No single agency is responsible for all matters regarding financial data governance, but the CFPB must deal with it under its own mandate. The CFPB is entrusted with enforcing federal consumer financial law to ensure that all consumers have "access to markets for consumer financial products and services and that markets for consumer financial products and services are fair, transparent, and competitive."¹⁸ The Bureau is authorized to exercise its authority to ensure consumers are:

- (1) provided with timely and understandable information to make responsible decisions about financial transactions;
- (2) protected from unfair, deceptive, or abusive acts and practices and from discrimination;

Due its position at the "user interface" of the financial system, the CFPB is particularly well disposed to lead the way on financial data governance.¹⁹ Financial datastreams often begin at the household level and are aggregated, disaggregated throughout the broader financial system, including capital markets.

The CFPB offers an example of an agency that avoids some of the major potential institutional challenges that other regulators might face: susceptibility to capture, a lack of technological sophistication, and insufficient authority. The CFPB embraced its identity as a 21st century, data-driven, technologically capable agency from the outset.²⁰ The CFPB hired a large number of computer engineers before becoming operational and has developed a suite of online digital tools for consumers.²¹ Compared to the FTC, the CFPB has more authority to write rules, impose civil penalties, and supervise data collection.²² More generally, it has the authority and power to meet the task of watching the watchers, ensuring consumer financial data is secure and bounded.²³

¹⁷ For timely legal analysis of data aggregators' relationships with banks, tech companies, and consumers in the context of Section 1033, see generally Nizan Geslevich Packin, *Show Me the (Data About the) Money!*, 2020 Utah L. Rev. 1277, 1288 (2020).

¹⁸ 12 U.S.C. § 5511.

¹⁹ See 12 U.S.C. § 5495 (noting the Bureau shall coordinate with other regulators).

²⁰ K. Sabeel Rahman, *Envisioning the Regulatory State: Technocracy, Democracy, and Institutional Experimentation in the 2010 Financial Reform and Oil Spill Statutes*, 48 Harv. J. Legis. 555, 557 (2011).

²¹ Rory Van Loo, *Technology Regulation by Default: Platforms, Privacy, and the CFPB*, 2 Geo. L. Tech. Rev. 531, 532 (2018).

²² *Id.* at 531–32.

²³ See Rory Van Loo, *Rise of the Digital Regulator*, 66 Duke L.J. 1267 (2017) ("The unpleasant truth is that creating effective digital regulators would require investing heavily in a new oversight regime or sophisticated state machines.")

Consumer Financial Protection: From Market Power to Platform Power

Financial data collection has changed significantly since the passage of the Dodd-Frank Act. Technology companies entering the space are subject to far less regulation than traditional financial institutions.²⁴ It is now critical for policymakers to understand *platforms*: entities that generate and intermediate market activity by generating and intermediating data.²⁵ On its face, longstanding institutions in the financial system, including credit reporting agencies, fit this description. But analysis of payments and credit data increasingly represents a logical extension of the Silicon Valley platform business model.²⁶

From the perspective of users, platforms make certain services more accessible or convenient. Platforms deploy additional services that expand the user base and yield more information, helping the platforms continually accumulate profits and power.²⁷ In a fashion familiar to financial regulators, dominant platforms produce “tranches” of data with corresponding predictive profiles, which they use to sell products to their users.²⁸ However, platforms also use these tranches for targeted advertising — essentially, to sell *access to their users* to third parties. Like mortgagors whose claims are bundled into mortgage-backed securities, surveilled users have no control over how our inputs are used for downstream products.²⁹ In one way or another, the platforms use our data to manufacture wealth for themselves.³⁰ Meanwhile, there is mounting evidence that commercial surveillance amplifies organized hate, junk science, and virulent nationalism, creates novel and potent pathways for discrimination, and generally facilitates unprecedented infringement of our rights to privacy, freedom of expression, and freedom of association.³¹

Among the network of platforms that increasingly define modern financial services are “data aggregators.” When consumers use online banking and fintech apps (like Venmo) they are likely providing account information to data aggregators. In the U.S., roughly 50% of U.S. consumers are estimated to have signed up for financial apps or other products that frequently rely on data aggregators to collect information via authorized transfers.³² The aggregation system is thought to reach about 95% of U.S. deposit accounts, and at least one aggregator estimates that it alone has connected to one in four financial accounts in the U.S.³³

²⁴ See Kristin Johnson, Frank Pasquale & Jennifer Chapman, *Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation*, 88 Fordham L. Rev. 499, 505 (2019) (discussing the gaps in the supervision of FinTech companies and how that encourages them to engage in regulatory arbitrage).

²⁵ See COHEN, *supra* note 2, at 37-47 (2019) (outlining and discussing the historic transition from market-based to platform-based business activity).

²⁶ Platforms organized through the logic of networks provide “would-be counterparties with *access* to one another and techniques for rendering users *legible* to those seeking to market goods and services to them.” *Id.* at 74, 182-187.

²⁷ See, e.g., BANK FOR INT’L SETTLEMENTS, BIS ANNUAL ECONOMIC REPORT 2019 62-64 (2019), <https://www.bis.org/publ/arpdf/ar2019e3.htm> [hereinafter BIS REPORT]; WILSON C. FREEMAN & JAY B. SYKES, CONG. RESEARCH SERV., R49510, ANTITRUST AND “BIG TECH” 10 (2019), <https://fas.org/sgp/crs/misc/R49510.pdf>.

²⁸ See COHEN, *supra* note 2, at 69.

²⁹ *Id.* at 73.

³⁰ *Id.* at 70-73.

³¹ *Id.* at 92, 239-250.

³² Geslevich Packin, *supra* note 17, at 1286-87.

³³ Zack Meredith & Zeya Yang, Blog, The All-New Plaid Link, Plaid (Oct. 2, 2020); Michael Deleon, A Buyer’s Guide to Data Aggregation, Tearsheet (Feb. 19, 2019).

Frequently, the data aggregator stores the login credentials of consumers and uses them to continually log into the consumer's bank account to copy all personally identifiable data, ranging from transaction information to account numbers. Once it has accessed consumer data, the data aggregator can share or sell that data without the consumer's knowledge, much less consent.

Even though they are not new entities,³⁴ as Nizan Geslevich Packin argues in a timely law review article, companies like Plaid, Intuit, Finicity, Envestnet|Yodlee, Morningstar/ByAllAccounts, Fiserv/CashEdge, and MX are “barely subject to any regulation, have received little scholarly attention, and most consumers have never even heard of them or know what they do.”³⁵

Data Security

More than 4,000 known data breaches have shaken markets during the last decade.³⁶ Data aggregators and all other companies share blame for breaches and hacks that have plagued consumers in a generally insecure system. As consumer advocates have long noted, the credit bureaus' loose matching procedures contribute significantly to the problem of identity theft. However, the general lack of regulation over data aggregators, means that if fintech apps have exploitable vulnerabilities, then the login credentials of accounts, including traditional bank accounts, could be jeopardized. Banks have maintained that if consumers share their credentials with third-parties and fraud takes place, liability protections like Regulation E--establishing the rights, liabilities, and responsibilities of participants in electronic fund transfer systems--will not be available for consumers.³⁷

There is no federal law creating uniform nationwide standards for alerting consumers about data breaches or for providing simple dispute solving mechanisms. Since 2002, the FTC has exercised its authority over security in this space, but because its power is restricted to enforcement action, the agency cannot supervise or examine nonfinancial companies on an ongoing basis. All businesses are subject to state laws, but these laws are few and ineffective.³⁸

FinTech companies' data gathering is typically done by one of two ways: (i) screen-scraping of public data from a website and (ii) APIs, a technology that enable programmers to integrate data from one source into third-party apps, restrict how apps tap data, and contractually limit the data's usages. Industry participants believe that the most dangerous type of data sharing is done via screen-scraping because data aggregators extract transaction information to populate their services and store and maintain the credentials, sometimes even after the relationship with the consumer ends. At least some consumer

³⁴ See generally Kimberly L. Wierzel, *If You Can't Beat Them, Join Them: Data Aggregators and Financial Institutions*, 5 N.C. Banking Inst. 457 (2001) (explaining that data aggregators enable consumers to turn over their different accounts' login credentials at various banks to one operator, which in turn lets them view all of their data from one site).

³⁵ Geslevich Packin, *supra* note 17, at 1286-1286.

³⁶ *Examining the Use of Alternative Data in Underwriting and Credit Scoring to Expand Access to Credit: Hearing Before the Task Force on Fin. Tech. of the H. Comm. on Fin. Serv.*, 116th Cong. 14 (2019) (statement of Kristin N. Johnson, Professor, Tulane Univ. L. Sch.).

³⁷ Geslevich Packin, *supra* note 17, at 1302-03.

³⁸ *Id.* at 1326.

groups agree that data aggregators' screen-scraping practices must be legally prohibited.³⁹

Data Privacy

No overarching federal privacy law currently curbs the collection, use, and sale of personal data among corporations.⁴⁰ Millions of people are subject to data collection to which they may not have meaningfully consented. This is especially true in the payments space, where counterparties between networked payment “stacks” are constantly exposed to each other.

For purposes of financial privacy, FCRA remains the most relevant statute. Yet FCRA was drafted before concentrated computerized data sharing became the standard industry business model.⁴¹ FCRA restricted data procurement to “a legitimate business need.” Companies have easily argued that direct mail and targeted advertising programs constitute legitimate business needs.

Of course, the *commercial* sharing and selling of predictions about human behaviors is only one dimension of payments technology and surveillance. We tend to obscure how the government itself is a financial data collector.⁴² According to Virginia Eubanks, social welfare agencies turned to cost-cutting technologies in periods of austerity.⁴³ The “digital poorhouse” was erected to stand between recipients of public assistance and their rights. Payments technology is a significant part of this story, as account-based Electronic Benefits Transfer (EBT) cards have granted agencies unparalleled and unprecedented supervision over the finances of people receiving SNAP, Housing Assistance, Supplemental Security Income, Medicaid, and more. Increased surveillance compounds the violence inherent to more traditional forms of finance. As Angela Harris argues, a spectrum of “slow violence”—the “sprawling system of surveillance, punitive discipline, and control that makes the lives of poor people profoundly unfree” dominates the “mundane world” of misdemeanor convictions, accompanies a similarly humdrum world of “payday loans, credit cards with ruinously high interest rates, for-profit colleges, and of course subprime mortgages.”⁴⁴ As I have discussed in previous testimony, the mass surveillance scheme attending AML, CFT, and sanctions law creates other racialized harms. Financial institutions must generally assist police investigations requiring financial information and provide specific information to law enforcement agencies, including by filing SARs. Payments data now have different lives in the law enforcement sphere.

It was once easier to imagine a notice-and-consent regime would allow individual

³⁹ See *Complaint, Cottle v. Plaid, No. 4:20-cv-03056-DMR (N.D. Cal. May 4, 2020)*.

⁴⁰ BERKELEY MEDIA STUDIES GROUP ET AL., *THE TIME IS NOW: A FRAMEWORK FOR COMPREHENSIVE PRIVACY PROTECTION AND DIGITAL RIGHTS IN THE UNITED STATES*, Citizen.org, (last visited Mar. 31, 2020), <https://www.citizen.org/sites/default/files/privacy-and-digital-rights-for-all-framework.pdf>.

⁴¹ Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 Md. L. Rev. 439, 442–43 (2020).

⁴² Marion Fourcade, Jeff Gordon (2020). Learning Like a State: Statecraft in the Digital Age. *Journal of Law and Political Economy*, 1(1). Retrieved from <https://escholarship.org/uc/item/3k16c24g>.

⁴³ VIRGINIA EUBANKS, *AUTOMATING INEQUALITY* 32-34 (2017).

⁴⁴ Angela Harris, *Criminal Justice and Slow Violence in Keilee Fant v. City of Ferguson, Missouri*, LAW & POL. ECON. (May 2, 2018), <https://lpeproject.org/blog/criminal-justice-and-slow-violence-in-keilee-fant-v-city-of-ferguson-missouri/>.

internet users on how to manage trade offs between convenience and privacy.⁴⁵ Managing how one's data is collected and used is now virtually impossible to do comprehensively. The best people can do is manage their privacy haphazardly.

Fair Competition

Unregulated surveillance may also spoil competition. Dominant platforms grow by expanding their platforms' user base and information access, securing revenue by selling products directly to their users or by selling access to their users to third parties.⁴⁶ As U.S. legal scholars and European antitrust authorities have concluded, data begets market power, but market power also allows dominant platforms to continually extract data in unfair ways.⁴⁷ For instance, Amazon already provides the cloud-computing systems that serve as the "technological backbone" of many fintech firms, which grants Amazon access to data other companies are structurally unable to obtain.⁴⁸ The company could easily take advantage of this data to unfairly compete with its existing fintech business partners.

Increased attention is especially necessary as more traditional financial institutions, including banks, credit card companies, and credit reporting agencies jostle with data aggregators over control of consumer financial data and the law governing its use. There are many dynamics at play. For instance, as antitrust advocates argue for open banking, data sharing appears to cut against the trend in the industry towards data privacy. In recent years, regulators have increasingly pushed financial institutions to strengthen their authentication procedures and cybersecurity processes in order to ensure that hackers do not gain unauthorized access to customer data.⁴⁹

The API approach may fundamentally leave traditional financial institutions in the drivers' seat. If not approached thoughtfully, regulators history demonstrates that open access and interoperability requirements can actually serve as instruments by which dominant firms obtain and entrench their monopoly power.⁵⁰ Allowing users to interact with banks as platforms by incorporating APIs would allow third-parties to plug straight into the relevant code and data feeds. However, with additional regulatory guidance, API access could be limited to specific types of information and sharing.

⁴⁵ See Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH. L. REV. 1 (2021). Cf. Cohen, *supra* note 11, at 386 ("[C]urrent consumer protection paradigms framed in terms of notice and choice are ill-suited to address these issues, which are fundamentally issues of economic and social inclusion.")

⁴⁶ See, e.g., BANK FOR INTERNATIONAL SETTLEMENTS, *supra* note 27.

⁴⁷ Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 518 (2019).

⁴⁸ John Detrixhe, *Amazon is invading finance without really trying*, QUARTZ (Nov. 1, 2017), <https://qz.com/1116277/amazons-aws-cloud-business-is-reshaping-how-the-financial-services-industry-works/>

⁴⁹ Cesare Fracassi & William Magnuson, *Data Autonomy*, 74 VAND. L. REV. 327, 349–53 (2021).

⁵⁰ "Our paper tells the untold story of how the SEC's attempt to promote competition in US securities clearing and depository markets through mandated interoperability ultimately paved the way for the DTCC's current monopoly over these systemically important markets." Awrey, Dan and Macey, Joshua, *Open Access, Interoperability, and the DTCC's Unexpected Path to Monopoly* (July 12, 2021). Available at SSRN: <https://ssrn.com/abstract=3885194> or <http://dx.doi.org/10.2139/ssrn.3885194>.

CFPB Recommendations

CFPB Section 1033 Rulemaking Should Promote Consumer Control in the Context of Data Minimization

In October 2017, the CFPB released a set of non-binding principles on the use of financial data.⁵¹ In particular, the principles permit consumers to “authorize trusted third parties to obtain” their data “from account providers to use on behalf of consumers, for consumer benefit, and in a safe manner. The principles also provide guidance for third-party providers of services, stressing issues such as protecting consumers’ data from security breaches, obtaining clear and informed consent from consumers, and limiting access to data. Yet the principles provided little clarity on key issues, including whether Section 1033 preserves third-parties’ right to pull data directly from bank customers’ accounts.

On its face, 1033 is a disclosure rule. Subject to rules prescribed by the Bureau, financial institutions must make available to a consumer information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data.⁵²

The Bureau’s rule may require financial institutions to make available to a consumer information relating to any transaction, series of transactions, or to the account including costs, charges and usage data.⁵³ Herein the Bureau should clarify their rights under the Electronic Funds Transfer Act (EFTA) as implemented by Regulation E (Reg E). Two areas need particular attention. In addition to establishing rights and responsibilities of providers, the Bureau should clearly enumerate what data is included in 1033 access rights, and should strictly prohibit the collection of certain data for any purpose.⁵⁴

Sometimes overlooked is the duty of the Bureau to prescribe or promote standardized formats for information to be made available to consumers under this section.⁵⁵ Arguably, this provides the Bureau with something like entry restriction power: if companies cannot comply with 1033 by providing an accurate record of data usage per the terms of the rule, they should be deemed to be out of compliance with 1033 and penalized thoroughly. The Bureau’s rulemaking may also standardize how consumer financial information is disclosed and at what level of understandability. The current disclosures required by the GLBA, which are intended to give consumers the opportunity to opt-out of the sharing of nonpublic personal information with third parties and to outline the company’s data use practices, are so confusing that consumers are unlikely to exercise their rights.⁵⁶

⁵¹ CFPB, Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation (2017) [hereinafter CFPB Consumer Protection], https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf [<https://perma.cc/OE69-87KQ>].

⁵² 12 USC 5533.

⁵³ *Id.*

⁵⁴ Christina Tetreault, Comments to the CFPB re Consumer Access to Financial records, https://files.consumerfinance.gov/f/documents/cfpb_tetreault-statement_symposium-consumer-access-financial-records.pdf.

⁵⁵ 12 USC 5533(d).

⁵⁶ Statement of Travis Plunkett, Legislative Director, Consumer Federation of America on Behalf of the

FCRA Rulemaking Should Cement the Bureau's Authority over Data Aggregators

FCRA is also centered around disclosure. Any CFPB rulemaking in this space should impose such criteria and establish minimum procedures to ensure maximum possible accuracy. Just as importantly, the scope of FCRA must be redefined. We must apply FCRA rights to information data aggregators have for consumers who are permissioning data access for FCRA purposes. However, any Bureau rulemaking in this area should also remove any doubt that financial data aggregators are subject to FCRA. If FCRA is to make any sense by its own legislative logic, it should be expanded to encompass alternative reporting systems.

The text of FCRA includes recursive definitions of "consumer reporting agency" and "consumer report" -- consumer reports are communications of credit-related information by consumer reporting agencies. There are a number of open questions as to whether data aggregators and other new intermediaries qualify as consumer reporting agencies.⁵⁷ Despite the FCRA's very broad definitions of "consumer report" and "consumer reporting agency," circuit courts have recently shown a reluctance to respect the FCRA's plain language and its expansive coverage. These cases have undermined FCRA protections with respect to its scope of coverage. For example, the *Zabriskie* decision has provided support to certain types of specialty CRAs, such as criminal background check and tenant screening agencies, that claim they are not covered by the Act because they merely provide software to end users.⁵⁸

Like most consumer advocates, I agree it is essential that if these recommendations result in separate systems for FCRA and non-FCRA rights, that rules do not undermine FCRA coverage. If there is a controversy as to whether certain data qualifies as a "consumer report," for instance in the context of 1033 rulemaking, regulation should explicitly provide nothing in it shall be construed to limit or restrict the applicability of the FCRA.

CFPB Rulemaking Should Grant the Bureau Authority to Supervise Data Aggregators

Consumer advocates have argued the CFPB should promulgate a rule authorizing it to supervise all "data aggregators" for compliance with consumer financial protection laws.⁵⁹

Consumer Federation of America, Consumers Union, and the U.S. Public Interest Research Group, before the U.S. Senate Comm. on Banking, Housing, and Urban Affairs (July 13, 2004), available at <https://www.govinfo.gov/content/pkg/CHRG-108shrg26700/html/CHRG-108shrg26700.htm>.

⁵⁷ Under the FCRA, information that nominally suits as a "consumer report" will not trigger the Act's requirements unless it is provided by an entity meeting the definition of a "consumer reporting agency" ("CRA"). See 15 USC § 1681a(f).

⁵⁸ In *Zabriskie v. Federal National Mortgage Association*, 912 F.3d 1192 (9th Cir. 2019), a divided panel of the Ninth Circuit held that Fannie Mae, which licenses its proprietary software program known as Desktop Underwriter to lenders, is not a CRA because its role is purportedly limited to providing this software that in turn allows lenders to assemble or evaluate information.

<https://library.nclc.org/data-gatherers-evading-fcra-may-find-themselves-still-hot-water>

⁵⁹ See, e.g., EDITH RAMIREZ ET AL., FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY i-ix (2014), available at http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf?utm_source=govdelivery (suggesting the CFPB could define "large data brokers" as subject to its examination authority under 12 U.S.C. § 5514(a)(1)(B)); *Banking on Your Data: The Role of Big Data in Financial Services: Hearing Before the H. Comm. on Fin. Services*, 116th Cong. 20-21 (2019) (Statement of Lauren Saunders, Assoc. Dir., Nat'l Consumer Law Center), available at

Under existing privacy and data protection laws, such supervision only entails compliance with the aforementioned disclosure, notice-and-consent, and minimal information security rules, but 1033, FCRA, or UDAAP rulemakings could all augment the power of supervision.

As a condition of secure data management, the Bureau should insist that credit reports should be frozen by default to prevent identity theft and give consumers more control over their credit reports. The switch for access to our credit reports should automatically be set to “off.”

Through its supervision power, the Bureau can also take the lead on algorithmic accountability. Rory Van Loo argues the CFPB has the clear statutory authority to examine financial institutions' non-public data, even without suspecting any wrongdoing, through its supervision group.⁶⁰ Most importantly for present purposes, their examination manual specifies that examiners can review computer program and system details. A review of these highlight reports indicates that examinations sometimes unearth problems in regulated entities' source code.

It is possible that the Bureau's authority could reach major tech companies that have developed payment systems. Once a platform has taken in consumer financial data, the company's overall data security practices would arguably be relevant to any determination of whether Apple, Amazon, or Facebook sufficiently safeguard the financial data they collect.⁶¹

Additionally, if fintechs share or sell customer information with third parties (including data brokers), the CFPB could impose requirements on how those third parties use that information indirectly, by holding the entity that the CFPB regulates--the fintech or bank--accountable for what the third party does with the information.

In the platform era, the CFPB should monitor platforms to ensure those companies are respecting users' privacy.⁶² The information collected under these auspices can be limited to business data. Unlike crime agencies--which need users' identities to assess their personal targets--regulators are looking for wrongdoing by the business. They can analyze companies' internal policies and procedures, or even examine the code behind various algorithms, without obtaining any user data. Furthermore, for some harms requiring access to user accounts, it may be possible to provide the data to the regulator in de-identified form.

CFPB UDAAP Enforcement Should Center Unfair Data Collection

Should it find a violation of UDAAP or federal consumer financial law, the CFPB has broad enforcement powers.⁶³ It can not only use any remedies authorized by the individual enumerated consumer laws, but may also order “any appropriate legal or equitable relief” including, among other remedies, rescission of contracts, restitution, disgorgement, and civil money penalties. Against covered persons and service providers, it can issue cease-and-desist

<https://www.nclc.org/images/pdf/cons-protection/testimony-lauren-saunders-data-aggregator-nov2019.pdf> (arguing the same point).

⁶⁰ Van Loo, *supra* note 21, at 542–43.

⁶¹ *Id.*

⁶² *Id.*

⁶³ See Katherine M. Porter, *Modern Consumer Law* 171 (2016) (lauding the “flexibility” of UDAAP statutes because otherwise you leave legislatures to play “whack-a-mole”).

orders or obtain consent orders in settlement of those proceedings. And for both covered and non-covered persons, the Bureau has the discretion to proceed in federal district court or through its own administrative procedure process. Finally, the Bureau may prescribe rules identifying specific practices as unfair, deceptive, or abusive acts or practices.⁶⁴

The Biden Administration's inclusion of CFPB UDAAP authority in its recent Executive Order is welcome.⁶⁵ Section 1033 rulemaking and other changes should be considered alongside a tougher enforcement strategy. The CFPB could pursue its mission by bringing enforcement actions directly against financial institutions, tech companies providing financial services, and third-party service providers including data aggregators. In particular, the unfairness authority deserves increased attention.

A practice is “unfair” if it causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Bureau may consider established public policies as evidence to be considered with all other evidence.

Proving injury has become substantially more difficult in privacy and security cases in recent years. Rulemaking can clear this up. “Substantial injury” can include small harms inflicted on a large number of people.⁶⁶ More easily identifiable harms from flowing from financial data collection and sharing include cyber fraud, unauthorized transactions, and identity theft. If customers' credentials are jeopardized, they would be exposed to data and financial losses with very limited, if any, legal recourse. Similarly, focusing on the issue of credential sharing, banks have maintained that if consumers share their credentials with third-parties and fraud takes place, liability protections like Regulation E--establishing the rights, liabilities, and responsibilities of participants in electronic fund transfer systems--will not be available for consumers.⁶⁷

“Reasonably avoidable” focuses on whether consumers have reason to anticipate the impending harm and the means to avoid it. As discussed, consumers typically have no idea data aggregators are even collecting their data. Yet aggregators are often given access to consumer accounts per contractual agreements with a financial services provider, although they are not regulated like financial services providers.

Lauren Willis has argued that the exploitation of false consumer beliefs about facts material to a transaction is an unfair trade practice.⁶⁸ Exploiting these beliefs fits comfortably within the existing definition of unfairness. Given the extremely widespread use of deceptive dark patterns by major retailers and app sellers, the only way for consumers to avoid such materials today would be to refrain from online commerce, which would be an unreasonable

⁶⁴ 12 U.S.C. § 5531(b).

⁶⁵

<https://www.consumerfinancemonitor.com/2021/07/12/president-biden-issues-executive-order-encouraging-ftc-rule-making-on-consumer-data-collection-cfpb-rulemaking-on-data-portability-and-cfpb-udaap-enforcement/>

⁶⁶ See, e.g., *FTC v. Commerce Planet*, 878 F. Supp. 2d 1048, 1078 (C.D. Cal. 2012) (holding that a small monthly charge, when assessed on many misled consumers, can constitute “substantial injury” (citation omitted)).

⁶⁷ Geslevich Packin, *supra* note 17, at 1302-03.

⁶⁸ See Lauren E. Willis, *Deception by Design*, 34 Harv. J.L. & Tech. 115 (2020).

demand to place on consumers and would harm both consumers and competition. Unfairness doctrine would thus act as a prophylactic against deceptive trade practices.

Under Director Corday, the Bureau virtually always asserted its “abusive” authority alongside claims of an unfair or deceptive act or practice. To the extent that algorithmic lenders use their credit-scoring models to engage in predatory lending practices, especially via unsubstantiated claims about the use of artificial intelligence and machine learning in financial services, the CFPB should use its “abusiveness” authority to curtail those practices.⁶⁹

Congressional Recommendations

Congress Should Structurally Separate Commercial and Financial Power

Smart enforcement of Section 1033 could give consumers control over their financial data, which should make it easier for them to switch between banks and other financial institutions, which could make them less reliant on the nation’s largest and most politically powerful banks, the big three credit reporting bureaus, and Mastercard and Visa’s duopoly over payment processing.⁷⁰ Just as the CFPB opens the space for competition, though, legislators should reestablish a bright line between the ownership of large tech companies and the ownership of financial institutions. We need structural partitions between commerce and banking, profit-driven enterprise and “money creation”, and platforms and payment systems.⁷¹ Even smaller tech and fintech companies are now acquiring regulated banks.⁷²

Congress Should Constrain Data Usage to a Short List of Permissible Purposes

No overarching federal privacy law currently curbs the collection, use, and sale of personal data among corporations.⁷³ Congress should take action to minimize *all* data collection to that which is narrowly tailored to permitted usages.⁷⁴ However, in doing so, Congress must go beyond the notion of the notice-consent standard, where consumers are expected to decide to permit — or forbid — use of their data. This standard supports data collection, but fails

⁶⁹ Matthew Adam Bruckner, *The Promise and Perils of Algorithmic Lenders’ Use of Big Data*, 93 Chi.-Kent L. Rev. 3, 47–49 (2018).

⁷⁰ https://www.huffpost.com/entry/the-obscure-biden-administration-rule-that-could-help-americans-flee-big-banks_n_606e0dd0c5b6034a708417c9

⁷¹ See Letter from Ams. for Fin. Reform Ed. Fund and Demand Progress Ed. Fund to H. Comm. on the Judiciary (Apr. 17, 2020).

<https://ourfinancialsecurity.org/2020/04/joint-letter-promote-tradition-of-separating-banking-and-commerce-regarding-dominant-platforms/> (arguing for the structural separation of large tech platforms and payments).

⁷² See, e.g., Hugh Son, *LendingClub buys Radius Bank for \$185 million in first fintech takeover of a regulated US bank*, CNBC (Feb. 18, 2020).

<https://www.cnbc.com/2020/02/18/lendingclub-buys-radius-bank-in-first-fintech-takeover-of-a-bank.html>.

⁷³ BERKELEY MEDIA STUDIES GROUP ET AL., *THE TIME IS NOW: A FRAMEWORK FOR COMPREHENSIVE PRIVACY PROTECTION AND DIGITAL RIGHTS IN THE UNITED STATES*, Citizen.org. (last visited Mar. 31, 2020).

<https://www.citizen.org/sites/default/files/privacy-and-digital-rights-for-all-framework.pdf>

⁷⁴ In the FCRA, the term “permissible purposes” is also far broader than credit. Three of these purposes are for credit, insurance, or employment. But a permissible purpose also includes use for government benefits, licenses, and the FCRA “catch-all” purpose of a “legitimate business need for the information – (i) in connection with a business transaction that is initiated by the consumer, . . .” 15 U.S.C. § 1681b(a)(3)(F)(i). For more on these “permissible purposes,” see National Consumer Law Center, *Fair Credit Reporting* (9th ed. 2017), updated at www.nclc.org/library.

consumers, as they are frequently determined to have “consented” to mass data collection and unknown down-stream uses. The FCRA established essential accuracy requirements for the data used in credit assessment tools, but consumers and their advocates carry the full burden of identifying and disputing inaccuracies.⁷⁵ While consumers should certainly have a right to notice (and to appeal of inaccuracies), it is not reasonable to believe that if consumers are provided with better information to assist them in making the right decisions as consumers, we will have met the greater challenges of financial data governance.

Nearly 7 in 10 Americans think companies use personal data in ways they’re comfortable with — about the same number who admit they never or only sometimes read privacy policies.⁷⁶ The very notion of digital consent has been complicated by “dark patterns” and other technology platforms used to exploit limits in user cognition and understanding.⁷⁷ Consumers typically have no knowledge of what they are consenting to on the internet.⁷⁸ Many experts argue the existing notice-and-consent regime does nothing to curb commercial surveillance.⁷⁹ Definitionally, the notice-and-consent paradigm cannot empower people to protect their privacy because, when people agree to share data, they do not know what they are really revealing or to what end.⁸⁰ Critically, corporate and government actors frequently do not even know the purpose until *after* they analyze an aggregated data set and identify the proxies.

The appropriate approach is to create bright-lines with respect to data collection in the first place. Sen. Sherrod Brown’s Data Accountability and Transparency Act, released in discussion draft form in 2020, would prohibit most collection and sharing of personal data as its starting point.⁸¹ Data could only be used in ways stipulated in the law, wherein collection is limited to that which is “strictly necessary” for a permissible purpose, such as providing a service a consumer asked for — and no more. Not permitted: using data for alternate purposes, holding onto it longer than necessary to carry out the original purpose, or sharing it unless that’s needed for the original purpose. One goal of his bill is thus to disrupt the business models of targeted advertising firms. Yet it still leaves a place for ads based on the contents of an ongoing search, for instance.

This sort of bright-line approach appropriately shifts the burden of privacy protection

⁷⁵ Anidjar & Inbar Mizrahi-Borohovich, *supra* note 7, at 197.

⁷⁶ <https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/>

⁷⁷ See, e.g., Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1461-1478 (2019) (borrowing a definition of dark patterns as “tricks used in websites and apps that make you buy or sign up for things that you didn’t mean to.”). For instance, consent could be gained by inserting a clause in extensive terms and conditions. See, e.g., Thibault Schrepel, *Libra: A Concentrate of ‘Blockchain Antitrust’*, 118 MICH. L. REV. ONLINE 160, 166 (2020).

⁷⁸ Comment from Freedom from Facebook to FTC (Aug. 20, 2018).

https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0008-147767.pdf

⁷⁹ See, e.g., Nizan Geslevich Packin & Yafit Lev-Aretz, *Big Data and Social Netbanks: Are You Ready to Replace Your Bank?*, 53 Hous. L. Rev. 1211, 1279–81 (2016); Nathan Newman, *How Big Data Enables Economic Harm to Consumers, Especially to Low-Income and Other Vulnerable Sectors of the Population*, 18 J. INTERNET L. 11, 19 (2014).

⁸⁰ Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 Md. L. Rev. 439, 453–61 (2020).

⁸¹ See Press Release, Brown Releases Proposal to Protect Consumers Privacy, Jun. 18, 2020, available at <https://www.brown.senate.gov/newsroom/press/release/brown-proposal-protect-consumers-privacy/>.

away from consumers, who have minimal resources to protect themselves, and toward corporations, which profit immensely from the aggregation of our data. In a boon to security concerns, personal data would not be retainable beyond a period of time *strictly necessary* to carry out a permissible purpose. The bill's ban on discriminatory uses of personal data, and the safeguards it would put in place against unfair algorithmic decision-making, address serious and growing dangers to equity.

Passage of legislation of this type would mean that certain kinds of data would be prohibited at the point of generation. In addition to banning the collection, use or sharing of personal data unless specifically allowed by law, DATA 2020 bans the use of facial recognition technology and prohibits the use of personal data to discriminate in housing, employment, credit, insurance, and public accommodations (subject to minimal exceptions).

The bill aligns with the general idea that non-credit uses of credit reports and scores should be greatly limited. Policymakers, advocates, fintech companies, and the credit industry incumbents have all promoted alternative sources of data as the solution to credit invisibility.⁸² While there is promise in some forms of alternative data, there are also significant risks. A bad credit history is more harmful than no credit history, and alternative data will not mitigate racial wealth disparities. There is no good evidence for the use of credit reports in employment, and its use in rental housing and insurance is also highly problematic. Some data shows promise, other data is a mixed bag, and some data is harmful enough that it should not be used. According to NCLC, the collection of gas and electric utility data for credit scoring is likely net harmful. Rental and telecommunications data could be promising, but carry significant risks, including the replication of racial inequity. Finally, many consumer advocates have argued that medical data should not be collected for credit scoring purposes.⁸³

Given the racial injustices perpetrated by law enforcement, it is concerning that fintechs might collect more geolocation or biometric data.⁸⁴ Geolocation data revealed by payment histories is uniquely difficult to anonymize.⁸⁵ Privacy and racial justice advocates vehemently oppose the use of biometric tools like facial recognition technology, iris-scanning, and palm prints.⁸⁶ Facial recognition software is likely to mislabel or misrecognize members of racial

⁸² Consumer Financial Protection Bureau, Data Point: Credit Invisibles, May 2015, http://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf. See also Tamara K. Nopper, *Digital Character in the "Scored Society": FICO, Social Networks, and the Competing Measurements of Creditworthiness*, in CAPTIVATING TECHNOLOGY: RACE, CARCERAL TECHNOSCIENCE, AND LIBERATORY IMAGINATION IN EVERYDAY LIFE 170, 170-188 (Ruha Benjamin ed., 2019) (illuminating how scoring by fintech lenders construct 'digital character' in a manner that can be opaque and discriminatory).

⁸³ Consumer Fin. Prot. Bureau, Market Snapshot: Third-Party Debt Collections Tradelines Reporting, July 2019 ("More than half (58 percent) of total third-party debt collections tradelines were for medical debt alone"), https://files.consumerfinance.gov/f/documents/201907_cfpb_third-party-debt-collections_report.pdf#page=13.

⁸⁴ See, e.g., Letter from Demand Progress et al. to Leaders McConnell and Schumer, Speaker Pelosi and Leader McCarthy (July 1, 2020), https://s3.amazonaws.com/demandprogress/letters/2020-07-01_Facial_Recognition_Moratorium_and_Divestment_Letter_FINAL.pdf; Alfred Ng, *Facial recognition has always troubled people of color: Everyone should listen*, CNET (June 12, 2020), <https://www.cnet.com/news/facial-recognition-has-always-troubled-people-of-color-everyone-should-listen/>.

⁸⁵ See, e.g., Cahn & Giddings, *supra* note 6.

⁸⁶ See, e.g., *A Biometric Backlash Is Underway — And A Backlash To The Backlash*, PYMNTS (May 17, 2019), <https://www.pymnts.com/authentication/2019/biometric-backlash-privacy-law/>; *Mandatory National IDs and Biometric Databases*, ELECTRONIC FRONTIER FOUND., <https://www EFF.ORG/issues/national-ids> (last visited Apr. 25, 2020).

minority groups, especially Black Americans.⁸⁷ Overall, the general use of this kind of sensitive data not only increases the risk of predation by banks and civil liberties violations by governments, but security breaches by competitors and hackers.⁸⁸

Financial Inclusion in the Informational Economy

Many claims are made about the promise of Big Data to increase financial inclusion, but those claims fail to reckon with, much less solve, the systemic reasons people are left out or more accurately deliberately excluded. Too often, promises of technological empowerment yield “predatory inclusion” — a process whereby financial institutions offer needed services to specific classes of users, but on exploitative terms that limit or eliminate their long-term benefits.⁸⁹

“Access to credit” talk pervades the current discourse of financial rights and equality for low-income communities. However, as Abbye Atkinson has argued, in concert with community advocates, the notion that credit is a valid form of social provision for low-income Americans, however, is deeply flawed.⁹⁰ At its best, credit is a mechanism of intertemporal and intrapersonal redistribution. The problem of entrenched and enduring poverty that leaves people consistently unable to afford basic necessities cannot be addressed by a device that requires future prosperity and economic growth. Indeed, the mechanism is fundamentally extractive. Too often, discussions about financial access disparities focus on the choices and behaviors of individuals, or on the need to design “alternative products,” rather than on structural barriers that block poor people, immigrants, and people of color from mainstream financial institutions and systems. Atkinson highlights that this sort of rhetoric is popular in both political parties.⁹¹

The intensity of data collection in consumer finance demands reflection about the role of banking and credit in the economy. A bank account is not the answer to every problem; credit is not a cure for poverty. If we have learned anything from approximately 250 years of

⁸⁷ See, e.g., Victoria Burton-Harris & Philip Mayor, *Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart*, ACLU (June 24, 2020), <https://www.aclu.org/news/privacy-technology/wrongfully-arrestedbecause>.

⁸⁸ See, e.g., Jason Leopold & Jessica Garrison, *US Intelligence Unit Accused Of Illegally Spying On Americans' Financial Records*, BUZZFEED (Oct. 6, 2017), <https://www.buzzfeednews.com/article/jasonleopold/US-Intelligence-unit-accused-of-illegally-spying-on> (reporting that FinCEN employees have accused colleagues at the Office of Intelligence and Analysis of illegally collecting and storing private financial records); Aaron Mackey & Andrew Corker, *Secret Court Rules That the FBI's "Backdoor Searches" of Americans Violated the Fourth Amendment*, ELECTRONIC FRONTIER FOUND. (Oct. 11, 2019), <https://www EFF.ORG/deeplinks/2019/10/secret-court-rules-fbi-is-backdoor-searches-americans-violated-fourth-amendment>; Chen Han & Rituja Dongre, Q&A. *What Motivates Cyber-Attackers?*, TECH. INNOV. MGMT. REV. 40, 40-41 (2014), <https://timreview.ca/article/838> (describing economic motivations for hacking).

⁸⁹ Louise Seamster & Raphaël Charron-Chénier, *Predatory Inclusion and Education Debt: Rethinking the Racial Wealth Gap*, 4 SOC. CURRENTS 199, 199-200 (2017) (describing the targeting of mortgagors and students who borrow to purchase homes or education as “predatory inclusion.”). Keeanga Yahmatta-Taylor uses “predatory inclusion” in the housing context - “[T]he turn to inclusion was only allowable by maintaining other forms of exclusion. Credit inclusion became possible by holding the line on neighbor exclusion. KEEANGA YAHMATTATAYLOR, RACE FOR PROFIT: HOW BANKS AND THE REAL ESTATE INDUSTRY UNDERMINED BLACK HOMEOWNERSHIP 254 (2019). See also Kristin Johnson et al., *Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation*, 88 FORDHAM L. REV. 499, 505, 517-21 (2019) (arguing fintech firms may “hardwire predatory inclusion” into financial markets for the “next several generations”).

⁹⁰ Abbye Atkinson, *Rethinking Credit As Social Provision*, 71 STAN. L. REV. 1093, 1093-94 (2019).

⁹¹ *Id.* at 1093.

U.S. governance of money, banking, and finance, it is that we shouldn't trust business (or government agencies) just because they claim to have new technologies that obviate the need to comply with the law. We do not trust claims of privacy, security, or stability merely when they are asserted by people who stand to benefit lucratively from the blind acceptance of promises. At the product, firm, or systems level. That would be imprudent and poor stewardship over the machinery at the center of our broader economy.

Even more importantly, we should not consign everyday people to accepting unnecessary and dangerous invasions of their privacy in order to participate in the financial system.

Financial technology can provide great benefits to society, but only if shaped by policymakers' own forward thinking about services people need in an informational economy.⁹² Policymakers must avoid being swayed by general promises of 'innovation' and create systems for real accountability on behalf of the public.

⁹² In previous testimony, I have urged Congress to establish privacy-respecting public options for real-time payments, safe deposits, international money transfer, and other basic digital financial services, as well as ensuring affordable, reliable internet access for these services to work. Public sector innovation is necessary to truly regulate the space, and privacy and public sector innovation need not conflict. See, e.g., *License to Bank: Examining the Legal Framework Governing Who Can Lend and Process Payments in the Fintech Age*, Hearing Before the Task Force on Financial Technology of the Committee on Financial Services, 116th Cong. (Statement of Raúl Carrillo, Policy Counsel, Demand Progress Education Fund & Fellow, Americans for Financial Reform Education Fund), <https://www.congress.gov/116/meeting/house/111057/witnesses/HHRG-116-BA00-Wstate-CarrilloR-20200929.pdf>.



House Financial Services FinTech Task Force

“Preserving the Right of Consumers to Access Personal Financial Data”

FinRegLab Testimony

Good morning. Thank you for the opportunity to testify before you today at the FinTech Task Force hearing, “Preserving the Right of Consumers to Access Personal Financial Data.”

My name is Kelly Thompson Cochran. I am the Deputy Director of FinRegLab, a D.C.-based independent, nonpartisan research organization that evaluates the use of new technologies and data to drive the financial services sector toward a responsible and inclusive marketplace. Through our research and policy discourse, we facilitate collaboration across the financial ecosystem to inform public policy and market practices.

FinRegLab has focused on issues concerning customer data access since the launch of our first empirical project in 2018, which evaluated the use of cash-flow data from bank accounts and other sources in underwriting consumer and small business credit.¹ We structured our work as a case study of the potential for customer-directed data transfers to spur greater competition and innovation in financial services, and concluded the project last year by publishing a policy analysis of how various stakeholders could help to strengthen financial inclusion and borrower protections in the broader ecosystem.² In partnership with the Financial Health Network, Flourish, and Mitchell Sandler, we also published a report that describes existing U.S. federal law governing consumer financial data and highlights open issues, areas of ambiguity, and other emerging topics.³ We also partnered with the Federal Reserve Bank of San Francisco in 2019 to host a symposium on the Role of Consumers in the Data Ecosystem⁴ and were invited to

¹ FinRegLab, The Use of Cash-Flow Data in Underwriting Credit: Empirical Research Findings (2019) (hereinafter, Cash-Flow Empirical Research Findings), https://finreglab.org/wp-content/uploads/2019/07/FRL_Research-Report_Final.pdf.

² FinRegLab, The Use of Cash-Flow Data in Underwriting Credit: Market Context & Policy Analysis (2020) (hereinafter, Cash-Flow Market Context & Policy Analysis), https://finreglab.org/wp-content/uploads/2020/03/FinRegLab_Cash-Flow-Data-in-Underwriting-Credit_Market-Context-Policy-Analysis.pdf.

³ Financial Health Network, Flourish, FinRegLab & Mitchell Sandler, Consumer Financial Data: Legal and Regulatory Landscape (2020) (hereinafter, Legal and Regulatory Landscape), <https://finreglab.org/wp-content/uploads/2020/10/Financial-Data-White-Paper.pdf>.

⁴ The symposium informed our 2020 cash-flow report as well as a report by SFFRB staff, Kaitlin Asrow, The Role of Individuals in the Data Ecosystem: Current Debates and Considerations for Data Protection and Data Rights in the United States, Federal Reserve Bank of San Francisco (2020).

participate in the Consumer Financial Protection Bureau’s 2020 symposium on consumer data access issues.⁵

Our research has focused most intensely on the use of customer-permissioned data for credit underwriting because credit has such important implications for broader economic participation, racial equity, and disaster recovery.⁶ However, customer-directed data transfers are also being used to support the provision of other financial services—including various payments and personal financial management applications—that could also have substantial benefits for historically underserved populations. Customer data access can also potentially facilitate the provision of financial services that are specifically tailored to meet the needs of small business owners.⁷

But manifesting these benefits is highly dependent on the commercial infrastructure that has developed to facilitate and use customer-permissioned data flows. Market activities and structures have expanded and evolved more quickly than U.S. regulatory frameworks over the last two decades, and action is needed by policymakers to calibrate competition and protection concerns to produce greater benefits from the system as a whole. We are encouraged to see regulatory activities by the Consumer Financial Protection Bureau, Federal Trade Commission, and prudential agencies that could help to address a number of critical questions. While additional work by industry and Congress will be needed to improve the broader data ecosystem, these regulatory initiatives are critical to help sharpen the focus of complementary efforts by other stakeholders and policymakers.

Why it matters: The potential scale, benefits, and risks of customer-permissioned data access

The generation of customer financial data has accelerated exponentially in recent decades as the financial services industry has come to rely heavily on digital information sources, back-office automation, and electronic service delivery. Financial services providers are also increasingly

⁵ We also submitted a comment in response to the Bureau’s Advanced Notice of Proposed Rulemaking on consumer data issues. <https://finreglab.org/wp-content/uploads/2021/04/FinRegLab-Section-1033-Comment-Letter-2021-1.pdf>.

⁶ Credit can not only help borrowers bridge short-term gaps, but fund long-term investments in housing, transportation, education, and small business formation. The credit system thus both reflects and influences the ability of families, small businesses, and communities to participate in the broader economy. For instance, historical discrimination in lending and other sectors has contributed to substantial racial disparities in income and assets, which in turn can affect household financial stability and the predictions of default risk that lenders rely upon to evaluate credit applications and set pricing. Cash-Flow Market Context & Policy Analysis §§ 2, 2.1, 2.2.

⁷ FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: Small Business Spotlight (2019) (hereinafter Cash-Flow Small Business Spotlight), <https://finreglab.org/wp-content/uploads/2019/09/FinRegLab-Small-Business-Spotlight-Report.pdf>; Karen G. Mills, Fintech, Small Business and the American Dream [eBook] (2019).

using information for marketing, verification, and other activities that is generated through their customers' interactions with other businesses, such as payroll services companies, merchants, and social media platforms. While traditional credit bureaus and payment networks have transferred customer data between financial services providers for decades, new types of intermediaries such as data aggregators and data brokers are becoming increasingly important hubs in this broader data ecosystem.⁸

The increasingly sophisticated use of data and technology could produce significant benefits for consumers and small businesses, for instance by increasing the speed and convenience of financial services delivery, expanding access for historically underserved populations, supporting more individually tailored financial products and services, and giving customers more control over their financial lives. However, changes in data and technology also require careful evaluation and management of risks, such as protections against data breaches and unauthorized transactions, the risk of replicating or re-enforcing historical discrimination, and potential losses of personal privacy and control.

The regulatory frameworks that govern the sharing and use of customer data by financial services providers have not kept pace with technology and market changes. While Congress adopted certain baseline privacy and information security requirements in 2000 and strengthened credit reporting protections in 2003, data sharing and usage practices have evolved significantly since that time.⁹ Moreover, while § 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act codified consumers' right to access their own data in 2010, the CFPB has not yet implemented that law or clarified the application of various existing protections to customer-directed data flows.¹⁰ The Bureau also has not yet taken steps necessary to begin examining larger data aggregators and other certain other non-bank data users for compliance with various federal laws.¹¹

⁸ Data aggregators emerged initially to support "personal financial management" services by collecting data from bank and investment firm websites, though they now support a broader array of financial services. Data brokers do not necessarily focus on financial data, though their information is used by many financial services providers for marketing and fraud detection. They collect and transfer information largely without consumers' knowledge or consent. Cash-Flow Market Context & Policy Analysis § 4.2; Legal and Regulatory Landscape at 12-13.

⁹ For background on the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act as amended by the Fair and Accurate Credit Transactions Act of 2003, see Legal and Regulatory Landscape at 46-106.

¹⁰ 12 U.S.C. § 5533. The Bureau issued non-binding principles regarding consumer data access in 2017 but did not start rulemaking activities until 2020. 85 Fed. Reg. 71,003 (Nov. 6, 2020); Consumer Financial Protection Bureau, Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation (2017).

¹¹ The Dodd-Frank Act authorizes the CFPB to examine non-bank lenders of any size that extend mortgages, private education loans, or payday loans, as well as "larger participants" in other markets after defining the relevant size thresholds by rule. 12 U.S.C. § 5514. The Bureau has set thresholds for consumer reporting, auto lending/leasing markets, and several other categories of financial services, but has not addressed data aggregators or other types of consumer loans.

Despite increasing concerns about U.S. regulatory infrastructure, the volume of customer-directed data flows—and of data sharing and use more broadly—continues to expand. Today, roughly 50% of U.S. consumers are estimated to have signed up for financial apps or other products that frequently rely on data aggregators to collect information via customer-authorized transfers, with substantial growth in the first months of the COVID-19 pandemic.¹² The traditional credit reporting system is even larger—with files on approximately 90% of U.S. adults—and impacts not only access to credit, insurance, and transaction accounts, but also employment and rental housing.¹³ Large financial technology companies are also increasing their involvement in financial services, acting as data sources, partners, and/or competitors to traditional providers.¹⁴

The resulting ecosystem is producing positive effects for many consumers and small businesses, but it is also imposing substantial burdens and risks that are reducing its ability to drive greater customer-friendly innovation and competition.¹⁵ As discussed below, competitive dynamics, coordination challenges, and regulatory uncertainty are substantially complicating the transition to safer and more reliable technologies for collecting customer-permissioned data. The lack of a consistent framework for data permissioning and protections also increases the burden on consumers and small businesses in managing how their data may be used and shared by a broad range of firms who participate in the provision of financial services.

¹² Aggregators are estimated to be able to access data from about 95% of U.S. deposit accounts, and at least one estimates that it alone has connected to one in four financial accounts in the U.S. Zack Meredith & Zeya Yang, Blog, The All-New Plaid Link, Plaid (Oct. 2, 2020); Michael Deleon, A Buyer's Guide to Data Aggregation, Tearsheet (Feb. 19, 2019). Firm estimates of how many consumers have authorized transfers are difficult to obtain because industry statistics are generally tracked on an account basis and surveys that focus solely on use of non-bank fintech services may count providers that do not rely on authorized data transfers and exclude banks that do use them. But growth trends are evident across multiple sources. See, e.g., Alexis Krivkovich et al., How US Customers Attitudes Toward Fintech Are Shifting During the Pandemic, McKinsey & Co. (Dec. 17, 2020); Karl Dahlgren, COVID-19 Pushes Digital Banking Adoption to the Tipping Point, BAI (Sept. 30, 2020); Plaid, The Fintech Effect: Consumer Impact and the Future of Finance (2020); EY, Global FinTech Adoption Index 2019 at 8 (2019); The Clearing House, Consumer Survey: Financial Apps and Data Privacy 2 (2019).

¹³ Cash-Flow Market Context & Policy Analysis § 2.2; Legal and Regulatory Landscape at 11, 81-106; FICO, Expanding Credit Access with Alternative Data 3 (2021). Data brokers, whose status as “consumer reporting agencies” under the Fair Credit Reporting Act depends on the intended use of their data, are also estimated to have information concerning nearly all U.S. consumers. Federal Trade Commission, Data Brokers: A Call for Transparency and Accountability 7-14 (2014).

¹⁴ See, e.g., Cash-Flow Small Business Spotlight § 4; Legal and Regulatory Landscape at 15; CBInsights, The Big Tech in Fintech Report (2021).

¹⁵ For in-depth discussions of the burdens and risks of the current market in connection with credit underwriting, see Cash-Flow Small Business Spotlight §§ 3-5; Cash-Flow Market Context & Policy Analysis §§ 3-6.

Addressing these issues could be particularly important to improving services to communities of color and other groups whose needs have not been fully met by either traditional financial services or early fintech initiatives:

- **Credit access:** Prior to the pandemic, an estimated 50 million consumers lacked sufficient traditional credit history to be evaluated using the most widely adopted credit scoring models, and an additional 80 million were rated as “nonprime” even though many of them individually may be likely to repay. Information barriers also substantially constrain credit access among small businesses. Research suggests that applicants of color, low-income households, and women entrepreneurs are disproportionately affected.¹⁶

FinRegLab’s 2019 empirical analysis of cash-flow information from bank transaction accounts and other sources suggests that the data could be valuable in predicting credit risk both among populations who lack traditional credit history and populations who do have credit scores, in part because the data appear to provide somewhat different insights than traditional credit reports.¹⁷ Our stakeholder outreach suggests that the information may be particularly valuable in detecting signals when economic circumstances are changing relatively rapidly or individual applicants are working to stabilize their finances. However, while interest in the use of such data is increasing particularly in the wake of the pandemic downturn, challenges in securing reliable data flows and uncertainty about applicable regulatory requirements remain significant obstacles to broader deployment.¹⁸

- **Tools to help manage debt, build savings, and meet other specific financial planning needs:** Although use of authorized data transfers to support personal financial management tools is far more widespread than in credit underwriting, many initial products were designed for and/or marketed primarily to relatively wealthy and

¹⁶ Cash-Flow Market Context & Policy Analysis § 2.2; Cash-Flow Small Business Spotlight § 2. Credit scoring models group borrowers into bands based on their relative default risk, but without additional data, lenders cannot differentiate within those bands to determine which individual applicants are higher-risk. Even if most applicants within a particular band are likely to repay their loans, lenders may choose not to lend to that cohort or may impose higher prices because default risks for the group as a whole are relatively high.

¹⁷ Cash-Flow Empirical Findings § 5. The study involved an independent analysis of data from six companies that use cash-flow information in lieu of or in addition to traditional credit bureau data to underwrite consumers or small businesses. The analysis also found evidence that the participating companies were extending credit to applicants who may have faced constraints in accessing credit historically, and that the degree to which the information was predictive of credit risk appeared to be relatively consistent across borrowers who likely belong to different demographic groups.

¹⁸ Cash Flow Market Context & Policy Analysis §§ 4-5; Cash-Flow Small Business Spotlight §§ 4-5; *see also* FinRegLab, Research Brief, Data Diversification in Credit Underwriting (2020).

technology-oriented consumers. Over time, some apps targeted to the needs of low-income households and other underserved populations have been developed by government agencies, nonprofits, and fintech companies.¹⁹ However, research suggests that additional product tailoring, outreach, and efforts to address concerns about data privacy and security could help to increase take-up rates.

For example, a project focusing on the high levels of high-cost debt among African-American households by Prosperity Now found some interest among research participants in using financial applications as a way to obtain tailored debt management advice.²⁰ However, in a user study of two apps, data flow issues proved to be a significant obstacle: Some participants were unwilling to set up account linkages due to identity theft and other risks, yet where manual data entry was an option they often did not enter sufficient data to generate the most valuable and tailored advice.²¹ Research by the Financial Health Network similarly suggests that both a lack of tailoring in product features and interfaces and the need to address information-related concerns have tended to reduce fintech take-up rates among low- to moderate-income consumers over 50, despite that population's rapidly increasing levels of digital connectedness and strong interest in both immediate financial management and retirement planning.²²

- **Payment services:** A number of digital payment services providers that are working to lower costs and/or increase convenience relative to traditional payment methods are using authorized data transfers via aggregators to facilitate their services. For instance, such data can be used to authenticate consumers' identities, confirm that consumer accounts have been properly linked to the apps, and check balances before processing a transaction over various types of payment rails. However, surveys suggest that at least with regard to so-called person-to-person payment services, usage is lower among African-American, Hispanic, and low-income households relative to white and higher-income households. In contrast, households of color and low-income consumers are more

¹⁹ See, e.g., Jeff Kauflin, Fintech Apps Offer Financial First Aid For Hardest-Hit Consumers, *Forbes* (Apr. 3, 2020); Financial Health Network, *Preparing for Tomorrow by Fixing Today: Helping Low- and Moderate-Income Americans Thrive in Retirement* (2018); MAV Foundation, *8 Mobile Apps That Can Help Low Income Families* (Mar. 14, 2018); Lucy Gorham & Jess Dorrance, *Catalyzing Inclusion: Financial Technology & the Underserved*, University of North Carolina Center for Community Capital 38-39 (2017); David Wessel, *Fintech Apps Bring Stability to Stressed Families*, *The Brookings Institute* (Apr. 25, 2017); Suman Bhattacharyya, *How Financial Tech Startups Are Reaching Out to Low-Income Americans*, *Tearsheet* (Feb. 10, 2017).

²⁰ Prosperity Now, *Overdue: Addressing Debt in Black Communities* 24, 27 (2018); Prosperity Now, *In Search of FinTech for Debt Management and Repayment* 25-26 (2020).

²¹ Prosperity Now, *In Search of FinTech for Debt Management and Repayment* at 5, 9-10, 14, 17, 19, 20-21.

²² Financial Health Network, *Fintech Over 50: Designing for Low- to Moderate-Income Older Adults* (2020); Financial Health Network, *Preparing for Tomorrow by Fixing Today* at 9-15.

likely than white and higher-income households to use non-bank providers of money orders, check cashing services, and bill payment services even though such options may carry relatively high fees.²³

Addressing these unmet needs will require more than just improving the efficiency and safeguards for customer-directed data flows—and the regulatory frameworks governing customer data use and sharing more generally. For example, improving digital connectedness and access to basic transaction accounts, targeted outreach and marketing, user-centric product design, and regulatory safeguards for the specific financial services at issue could also have significant effects on customer use of and confidence in various financial services. However, frictions in managing underlying data flows may have a particular impact on efforts to meet the financial services needs of underserved populations, for instance where providers' margins are already thin due to higher costs or lower returns,²⁴ or where particular customer groups are especially sensitive to concerns about privacy, security, and other aspects of data control.²⁵ Thus, improving the market and regulatory infrastructures for data sharing and use has critical implications for competition, customer protection, and financial inclusion going forward.

Current market and regulatory initiatives

The development of infrastructures supporting customer-directed data transfers is particularly significant within the broader ecosystem because they provide mechanisms for consumers and small businesses to use their data to obtain a range of products and services from additional financial services providers, in contrast to data flows that are provider-initiated. Development of the customer-permissioned system to date has been largely driven by competitive dynamics between the largest and most technically sophisticated companies. While recent efforts to develop technical standards and other mechanisms could potentially benefit smaller participants, competitive and coordination challenges remain substantial. Federal regulators could substantially boost these efforts by resolving certain threshold issues so that market participants can focus on remaining technical and process questions.

²³ Federal Deposit Insurance Corporation, *How American Banks: Household Use of Banking and Financial Services* 6-7, 37-38 (2020).

²⁴ For a discussion of how these factors affect bank efforts to serve non-prime populations, see *Cash-Flow Market Context & Policy Analysis* § 5.2.1.2.

²⁵ Although research specifically in the financial services context is limited, some surveys indicate that concerns about privacy may be higher among respondents of color and low-income households than the general population, in part due to lower trust in government institutions and business organizations. Brooke Auxier et al., *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control over Their Personal Information*, Pew Research Center (2019); Mary Madden, *Privacy, Security and Digital Inequality*, Data & Society Research Institute 2-10 (2017).

The customer-directed system started in the 1990s when aggregators began using customers' log-ins to banking and investment website platforms and automated programs to "screen scrape" data for use in various personal financial management applications. As the volume of activity rose to support an increasing range of financial services, many data holders reacted defensively in light of systems burdens, information security and liability concerns, and competitive tensions. Regulatory uncertainty has heightened some of these tensions, such as disagreements over how federal limitations on consumers' liability for unauthorized transactions would apply if their account log-in credentials are misused or breached in connection with a data transfer.²⁶ Uncertainty over the application of prudential regulators' guidance concerning bank oversight of third-party relationships has also complicated industry dynamics.²⁷

Against the backdrop of potential blocks to access (and sometimes actual shut-downs), large data holders have negotiated an increasing number of confidential bilateral agreements with individual aggregators to transition to read-only tokenized access, application program interfaces (APIs), and contractual limitations on data use and other topics. These newer technologies can increase the safety, accuracy, and efficiency of data transfers, but they have resource and competitive implications for the broader market. Screen scraping is frequently continuing to occur alongside API transfers, particularly where API limitations restrict the cadence or scope of available information.²⁸

Relying so heavily on contracts and due diligence mechanisms to police the broader data transfer system has other substantial drawbacks. Data holders may be direct competitors of the companies that are receiving the data from aggregators, and thus may have business incentives to impose restrictions on other ecosystem participants. Data intermediaries may not have the incentives or leverage to police the conduct of their clients across all potentially relevant issues.

²⁶ Cash-Flow Market Context & Policy Analysis §§ 4.2.3, 5.2.1.2; Legal and Regulatory Landscape at 152-171.

²⁷ Cash-Flow Market Context & Policy Analysis at 50; Legal and Regulatory Landscape at 107-122. After the U.S. Treasury Department suggested that some agency guidance was actually discouraging companies from entering agreements to move to safer data transfer technologies because banks feared the agreements would trigger heightened monitoring obligations, the Office of the Comptroller of the Currency issued guidance in 2020 stating that banks have due diligence duties even with regard to screen scraping activities by aggregators with which they have no contractual relationships. The guidance has created additional questions about the practical extent to which banks in such situations can gain sufficient assurances about aggregators' data controls and whether banks in certain circumstances have obligations to conduct "fourth party" monitoring of the data controls of aggregators' customers. U.S. Department of the Treasury, A Financial System that Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation 86-95 (2018); Office of the Comptroller of the Currency, OCC Bulletin 2020-10, Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29.

²⁸ Cash-Flow Market Context & Policy Analysis §§ 4.2.2, 5.2.2.1; Legal and Regulatory Landscape at 40-42.

And smaller companies face greater resource constraints in adopting new technologies, negotiating contracts, and conducting due diligence activities.²⁹

In light of these disadvantages, efforts to create standards and other infrastructure that can be used on a turnkey basis by a large number of participants have begun to attract increased interest from industry stakeholders in the past few years. For example, nearly 200 participants have joined the Financial Data Exchange to work on implementation of a common API, developing user experience guidelines to promote more consistent permissioning processes, and defining minimum data elements for particular use cases. The group includes a range of industry stakeholders, as well as some consumer advocate representation in its working groups. Other initiatives by several large banks and The Clearing House have both raised hopes that they will benefit smaller data holders and fears that they could be used to the founders' competitive advantage.³⁰

While industry-led standardization efforts can be critical to solving technical and process issues that may be both legally and practically difficult to enshrine in regulation,³¹ the experiences of the last several years suggest that such efforts will be far more effective if regulatory initiatives set certain basic parameters. For instance, even where consumer advocates have a seat at the table, it can be extremely difficult for voluntary private initiatives to establish and enforce consistent market-wide standards, particularly on topics that require careful balancing between the interests of multiple groups of consumers and financial services providers. More broadly, implementation and coordination costs remain serious challenges, and the COVID-19 pandemic has diverted substantial attention and resources to other issues. While FDX statistics indicate that the number of accounts using the FDX API for data transfers has increased to about 22 million, that represents only a small fraction of overall data transfer volume.³²

²⁹ Cash-Flow Market Context & Policy Analysis §§ 4.1.2, 4.2.2.

³⁰ Cash-Flow Market Context & Policy Analysis § 4.2.4; see also Penny Crosman, BofA, Chase, Wells Fargo Pilot Service to Rein in Screen Scraping, *Am. Banker* (Jan. 26, 2021).

³¹ Section 1033 directs the CFPB to develop rules that "prescribe standards applicable to covered persons to promote the development and use of standardized formats for information," but also to consult with other federal regulators to "ensure, to the extent appropriate, that [its] rules ... do not require or promote the use of any particular technology in order to develop systems for compliance." 12 U.S.C. § 5533(d), (e). The Bureau also lacks authority to set information security standards under GLBA. 15 U.S.C. § 6801(b). Even where legal authorities are clear, it can be challenging to keep rules that enshrine technical standards updated as technologies and market practices evolve. Cash-Flow Market Context & Policy Analysis § 5.2.2.1.

³² Financial Data Exchange, Financial Data Exchange (FDX) Reports 22 Million Consumer Accounts on FDX API (Sept. 1, 2021).

Setting clear regulatory baselines concerning the basic rights and protections for consumer data access could thus help to sharpen the focus of industry standardization initiatives. Three such agency initiatives are currently underway:

- **The FTC is considering a proposal to modernize information safeguard requirements for non-bank financial services providers under the Gramm-Leach-Bliley Act**, which could drive more robust data protections for intermediaries (including both traditional credit bureaus and data aggregators) and a wide range of non-bank data users.³³
- **The CFPB has issued an Advanced Notice of Proposed Rulemaking to seek input on implementation of § 1033.** The notice focused both on data access questions and on the treatment of consumer-permissioned data flows under other existing federal consumer financial protection laws, such as GLBA, the Fair Credit Reporting Act, and the Electronic Fund Transfer Act, though it did not focus extensively on supervision of data aggregators and other non-bank ecosystem participants.³⁴
- **The prudential banking agencies are seeking comment on harmonizing their guidance concerning third-party service provider obligations, including its application to customer-permissioned data transfers.** The notice seeks comment on whether the regulators should collectively adopt and/or revise guidance that the OCC issued in 2020 stating that banks have due diligence obligations even in situations in which they only have API agreements or no contractual relationships with data aggregators who are acting on behalf of competing financial services providers.³⁵

Yet while Executive Order 14036 recently encouraged the CFPB to proceed with a § 1033 rulemaking to “facilitate the portability of consumer financial transaction data so consumers can more easily switch financial institutions and use new, innovative financial products,”³⁶ several of these agencies are in leadership transitions and the scope and prioritization of these initiatives relative to other activities is not yet clear. We believe that the regulatory agencies could substantially strengthen the incentives for and efficiency of industry standardization efforts by providing a decisive answer to such core issues as:

³³ 84 Fed. Reg. 13158 (Apr. 4, 2019); Cash-Flow Market Context & Policy Analysis § 5.2.2.2; Legal and Regulatory Landscape at 71-81.

³⁴ 85 Fed. Reg. 71,003 (Nov. 6, 2020).

³⁵ 86 Fed. Reg. 38,182 (July 19, 2021); 86 Fed. Reg. 50,789 (Sept. 10, 2021); see supra note 25 and accompanying text.

³⁶ Executive Order 14036; Executive Order on Promoting Competition in the American Economy (Jul. 9, 2021).

- the deadline for particular groups of financial services providers to make data available upon consumer request under § 1033;
- the scope of data that is subject to § 1033 access rights or to exceptions under the statute, and whether data sources can impose other conditions before providing data access;
- the obligations of companies acting on behalf of an individual consumer in connection with a § 1033 data transfer and the requirements for data recipients to safeguard such information;
- the Bureau’s plans to begin supervision of data aggregators and possibly other categories of non-bank financial services providers that rely heavily on customer-permissioned data; and
- the scope of banks’ oversight responsibilities concerning activities of aggregators (or aggregators’ customers) in their downstream handling of customer data.

Interagency coordination is particularly important as these initiatives progress. For example, strengthening GLBA information safeguards requirements for all non-bank financial institutions and conducting CFPB examinations of data aggregators and other key actors could reduce the need to rely on bank oversight mechanisms to manage the broader ecosystem. And third-party service provider guidance can have important implications for competitive dynamics and the volume and nature of § 1033 data flows, for instance if heightened due diligence expectations disincentivize smaller institutions from entering agreements to manage and develop APIs to manage data transfers.

Revisiting the broader regulatory framework

In addition to sharpening the focus of future industry efforts, the agencies’ activities may also highlight the need for specific Congressional actions. For instance, § 1033 is focused primarily on retail financial products and services like loans and deposits, even though securities and insurance information could also be useful for personal financial management purposes.³⁷ The statute also does not affirmatively define protections for § 1033 data. Other existing federal laws provide potential safeguards, but they were not crafted specifically with the current customer-directed transfer system in mind and may not apply to all use cases.³⁸ And while the Bureau could potentially prescribe conduct requirements for companies who act as “agents” or

³⁷ 12 U.S.C. §§ 5481(5), (6), (15), 5517, 5519, 5533(a).

³⁸ For discussions of the protections provided by the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, and Electronic Fund Transfer Act and the questions and tensions raised by their potential application to customer-permissioned data flows, see Cash-Flow Market Context & Policy Analysis §§ 4.2.1.2, 5.2.2.2, 6.1.2, 6.1.3; Legal and Regulatory Landscape at 46-106, 152-171.

“representatives” on behalf of consumers in connection with § 1033 transfers,³⁹ it is unclear whether it will decide to do so or what such duties might entail.

Thus, Congressional action may well be required to help further strengthen and tailor the regulatory guardrails for customer-directed transfers. And even beyond those particular data flows, the gaps and disconnects between various federal consumer financial laws are becoming more problematic in light of the substantial evolution in industry players, technologies, and market practices over the last several decades. For instance, the GLBA privacy provisions that create some baseline limitations on when financial institutions can transfer data to other parties for their own purposes have not been substantially updated since their initial adoption, and raise substantial complexities as to the extent to which they limit data use and transfers by companies that receive the data downstream.⁴⁰ While U.S. law has historically provided more protection for customers’ financial data as compared to data in general commerce, gaps in the effectiveness and scope of those protections are becoming more important as data sharing and use within the financial sector continues to expand and as the boundaries between financial services and general commerce become more porous.

Several other nations and states are starting to adopt comprehensive regimes that create baseline rights and protections for customer data across all sectors, sometimes in combination with more tailored provisions to address customer protection and competition concerns in financial services.⁴¹ The potential conceptual and practical tradeoffs of different structures is beyond the scope of this testimony,⁴² but the need to modernize the regulation of customer data as used for financial services is becoming increasingly urgent. Several illustrations help to demonstrate this need:

- **Meaningful consent and its relation to meaningful protections.** Notice and consent concerning data access and use is a critical feature of today’s broader digital economy, but federal consumer financial laws often focus more on informing consumers about

³⁹ The Dodd-Frank Act defines “consumer” to include not only individuals but also “agent[s], trustee[s], or representative[s] acting on behalf of ... individual[s].” 12 U.S.C. §§ 5481(4), 5533(a). Thus, in determining application of § 1033, the Bureau could define what it means to “act on behalf” of an individual consumer. Under state law, for example, agents often have fiduciary duties to their principals, such as for instance by exercising appropriate care and diligence, acting within scope of delegated authority, and avoiding self-dealing.

⁴⁰ Cash-Flow Market Context & Policy Analysis at 96-101, 122; Legal and Regulatory Landscape at 48-70, 174.

⁴¹ For a detailed discussion of the intersections between data protections and data rights, see Asrow at 7-8, 11-12, 54-72. For summaries and discussions of other jurisdictions’ approaches to create comprehensive data regimes and to facilitate open finance systems relative to U.S. approaches, see Cash-Flow Market Context & Policy Analysis at 71; Asrow at 14-17, 52-53; Olivia White et al., *Financial Data Unbound: The Value of Open Data for Individuals and Institutions*, McKinsey Global Institute (2021).

⁴² See Cash-Flow Market Context & Policy Analysis § 7.3 for a brief discussion of selected issues.

product pricing and features prior to selection decisions rather than related data flows. Where prior consent is used to authorize transfers of consumer financial data, it often relies on “opt out” structures that may not be as effective in empowering consumers to exercise robust control over their data.⁴³

Section 1033 substantially increases the conceptual and practical importance of consent because it relies upon affirmative consumer opt-ins to data transfers. Adopting consistent, consumer-friendly disclosure content, formats and consent processes (particularly those designed for digital interfaces) will be important to effectuating the statute and realizing its larger benefits for innovation and competition.⁴⁴

But deeper thought about the nature of meaningful consent and its relationship with meaningful protections across the broader financial data ecosystem would also be helpful. Even with the adoption of best practices and model forms, there is growing evidence of “information overload” among consumers as they are asked to manage the use of their data while interacting with a broad range of entities in both financial services markets and general commerce. While some financial services providers are working to make this process more manageable by creating data dashboards and other best practices, it is difficult for individual commercial actors to overcome coordination challenges in gathering information from downstream parties. Setting regulatory baselines for traceability, the scope of permissible use activities, and other substantive data practices could also help to reduce cognitive burdens on consumers, for instance by reducing the number of issues that have to be managed on a company-by-company basis.⁴⁵

- **Access to data for research and development.** While § 1033 provides a right for individual consumers to access their data one financial services provider at a time, it does not address the fact that access to large pools of representative historical data can be critical for both product development (for instance, creation of more accurate and inclusive predictive models for credit underwriting) and research to inform improvements in market practices, public policy, and regulation. Existing laws such as GLBA and FCRA have been interpreted to provide more flexibility for research and

⁴³ Cash-Flow Market Context & Policy Analysis § 6.2.1; Legal and Regulatory Landscape at 43-44, 58-64, 92-94; Asrow at 22-29.

⁴⁴ Cash-Flow Market Context & Policy Analysis § 6.2.1; Legal and Regulatory Landscape at 43-44, 58-64, 92-94; Asrow at 22-29.

⁴⁵ Cash-Flow Market Context & Policy Analysis § 6.2; Legal and Regulatory Landscape at 58-64, 92-94; Asrow at 22-29, 30-35, 57-58, 63-66, 68-69.

development activities where data does not contain personally identifying information. However, new tensions between individual and collective interests are emerging as research highlights the risks of re-identification through linking of data sources and as notions of consumer control strengthen to include such concepts as a right to demand deletion.⁴⁶

New “privacy enhancing technologies” that reduce the possession and transfer of personal data while facilitating beneficial use cases may help to manage some of these tensions,⁴⁷ but policy frameworks may also need to be revised and recalibrated. For instance, the lack of access to data pools can substantially disadvantage startup financial services providers relative to incumbents that have already amassed substantial historical information. Thus, creating mechanisms that facilitate the development of products and services that will help consumers derive further benefits from their data could substantially increase § 1033’s potential benefits for innovation and competition.

- **The critical role of data intermediaries.** Data intermediaries often do not have direct relationships with consumers or small businesses but play increasingly important roles in the financial data ecosystem both as the repositories of information concerning millions of customers and as counterparties in an increasingly complex web of commercial relationships. Their activities and scale have important implications for both customer protection and competition, and different types of intermediaries are engaging with each other through both partnerships and acquisitions. Yet the extent to which different types of intermediaries are subject to direct regulation and supervision under current federal consumer financial laws varies. Third-party risk management authorities provide some additional protections, but they can be less comprehensive and efficient than direct regulation.⁴⁸

With regard to examinations, for instance, the Dodd-Frank Act vested the Consumer Financial Protection Bureau with authority to supervise non-banks that are “larger

⁴⁶ Cash-Flow Market Context & Policy Analysis § 6.1.3; Legal and Regulatory Landscape at 43-44, 55-57, 87; Asrow at 36-38, 59-60, 66-68.

⁴⁷ Cash-Flow Market Context & Policy Analysis at 100; Asrow at 75-77.

⁴⁸ Cash-Flow Market Context & Policy Analysis §§ 4.2.1, 4.2.4, 5.2.2.2; Legal and Regulatory Landscape at 9-13, 107-122. Under the Bank Service Company Act and Dodd-Frank Act, the prudential regulators and the CFPB can examine vendors to supervised financial service providers, in addition to the due diligence and monitoring conducted by the providers themselves. However, while prudential regulators have examined at least one data aggregator in its capacity as a vendor to a bank, they reportedly have disavowed such authority with regard to nationwide consumer reporting agencies. And because each supervised entity may interpret its due diligence obligations slightly differently, processes can be extremely duplicative for both banks and data intermediaries or other vendors.

participants” in markets other than mortgage, payday, and private student lending.⁴⁹ This excludes smaller intermediaries that may nonetheless aggregate the data of millions of consumers, simply because they are smaller than other competitors. Moreover, the Dodd-Frank Act did not authorize the CFPB to examine non-banks for compliance with GLBA information security requirements even when the agency is conducting other supervisory activities. The importance of this issue has been underscored by the Equifax data breach in 2017 and the increasing scale of data aggregators.⁵⁰

- **Treatment of small business owners.** Small business owners are not covered by § 1033 or most other federal consumer financial laws, yet they have substantial unmet needs for financial services.⁵¹ What research is available suggests that they are sensitive to many of the same data protection concerns as consumers.⁵²

The Consumer Financial Protection Bureau and other federal agencies can begin to tackle many of these questions with their existing authorities, but there are gaps and inconsistencies that they cannot bridge without action by Congress. Increasing the consistency and comprehensiveness of protections that apply to (1) different sources of data for credit underwriting; (2) customer-permissioned data transfers for all types of use cases; and (3) the use of customer data in financial services more generally would help to reduce risk levels to consumers and small businesses, create a more level playing field among financial services providers, and encourage customer friendly innovation and competition going forward. Such changes would not only increase the competitiveness of the U.S. financial system relative to parallel sectors in other countries, but increase the dynamism and competitiveness of our broader economy by helping historically underserved populations increase their economic participation, financial stability, and long-term wealth.

Conclusion

Some sources have estimated that broad adoption of open finance in the U.S. could add as much as 1.5% to the nation’s gross domestic product by 2030, including up to \$90 billion of economic

⁴⁹ 12 U.S.C. § 5514(a)(1)(B).

⁵⁰ Cash-Flow Market Context & Policy Analysis §§ 4.1.2, 6.3.2, 7.2; Legal and Regulatory Framework at 18-19, 73-75, 111-113.

⁵¹ Cash-Flow Small Business Spotlight §§ 2, 5; Mills Chapters 1-5, 9.

⁵² Barbara J. Lipman & Ann Marie Wiersch, Uncertain Terms: What Small Business Borrowers Find When Browsing Online Lender Websites, Board of Governors of the Federal Reserve System 23, 27 (2019); Barbara J. Lipman & Ann Marie Wiersch, Browsing to Borrow: ‘Mom & Pop’ Small Business Perspectives on Online Lenders, Board of Governors of the Federal Reserve System 12, 16-17 (2018); Barbara J. Lipman & Ann Marie Wiersch, Alternative Lending Through the Eyes of ‘Mom & Pop’ Small Business Owners: Findings from Online Focus Groups, Federal Reserve Bank of Cleveland 17 (2015).

value for individual consumers, \$50 billion for micro, small, and medium sized businesses, and \$100 billion for financial institutions.⁵³ But achieving such benefits will require sustained attention and action from industry, regulators, and Congress. The regulatory actions that are underway now are important steps down that path, and complex undertakings in their own right. They can help to sharpen the focus of subsequent standardization and legislative efforts, but fully modernizing the market and regulatory infrastructure that governs the use of customer data in financial services is an even larger undertaking that will require a sequencing of efforts by multiple stakeholders. The longer those efforts wait to start, the more risk that builds up in the system and the more benefits are forgone both in the financial sector and the broader economy. Thank you again for the opportunity to speak with you today about these important issues.

⁵³ White et al., at 10-11. The analysis calculates potential benefits from three potential benefits to customers (increased access to financial services, greater user convenience, and improved product options) and four potential benefits to financial institutions (increased operational efficiency, better fraud protection, improved workforce allocation, and reduced friction in data intermediation).

Testimony By
Steve Smith
Co-Founder and CEO, Finicity

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

Hearing Entitled
“Preserving the Right of Consumers to Access Personal Financial Data”

Tuesday, September 21, 2021

I would like to thank Chairwoman Waters, Ranking Member McHenry, Chairman Lynch, Ranking Member Davidson, and the Fintech Task Force for the opportunity to speak with all of you today. My name is Steve Smith, the Co-founder and CEO of Finicity, a Mastercard company.

Finicity allows financial account holders - typically consumers and small and midsize businesses - to easily connect their accounts to a wide range of financial apps and services. This is often called data aggregation.

I've spent the past 30 years working within the technology industry. In that time, there has been remarkable technological innovation. From the Internet, to mobility, to cloud computing, we've experienced massive advancements impacting virtually every industry. One notable technology disruption has been the use of data and analytics. Large enterprises have leveraged powerful data and analytics tools to gain insights on business operations, improve efficiency, enhance customer experiences and much more. All of this has enabled significant cost reductions combined with enhanced revenue opportunities.

For too long, we as individuals, families and small and midsize businesses haven't reaped the same benefits of using our data. Why? The technology has been too expensive or the ability to collect and analyze our data has been exceptionally difficult or cumbersome.

This is where the advent of open banking or open finance, powered by data aggregation, is flipping the data experience to one that empowers consumers and small and midsize businesses with access, control, and the consented use of their data.

Open banking is enabling a wide range of financial products and services that are transforming how consumers manage their money, prepare their taxes, apply for loans, make real-time payments, and better understand and improve their credit. All of this is leading to more consumer choice and better experiences, along with increased financial literacy, financial inclusion and improved financial fitness.

Finicity has been at the center of many of these empowering experiences. For example, we've enabled consumers to contribute more data to their credit scores through Experian Boost and the UltraFICO score. These solutions use cash flow data explicitly permissioned by users, to help them build or improve credit and achieve their financial goals.

So with all of this positive movement, why am I here? This is a technological shift that is still very much in its early innings. As it emerges and matures federal policymakers will play a meaningful role in the direction and pace of this transformation by providing clarity on data protection expectations, data privacy requirements and consumer data rights.

Clearly, consumer data protection is a must throughout the data access and sharing process. Safeguarding the data is foundational to accelerating innovation, while protecting the consumers from data theft.

Equally, I believe we all agree that the privacy of personally identifiable information is important to further consumer empowerment. In many respects, data privacy is about consent. With clear and explicit consent, consumers will know where, how and for what purpose their data is being used, putting them in control enhances privacy. Data should not be shared across or among organizations without direct and transparent consent.

Finally, and I think most importantly, consumer data rights must start and end with an individual's ability to access, use and benefit from their data. This is the foundation of open banking. It is essential that consumers have reasonable access to all of their financial data in possession of the data holders in a format that they can permission for use to financial services and app providers of their choosing. It is critical to safeguard data rights, otherwise the great progress we have made so far will fade.

Data rights, privacy and protection are inextricably connected policy goals. Each deserving focus and critical thinking. Trade-offs may have to be made to balance competing objectives. Even adopting newer and better technologies can have unintended consequences by curtailing data access. We should bear in mind that those three goals are not equal - the consumer's right to their data must always be the priority.

We need a clear regulatory framework to protect and continue open banking in the U.S. That is why we are encouraged by the CFPB finally moving forward on a rulemaking under section 1033 of the Dodd Frank Act.

When we started Finicity, we started with one simple thought: data is at the heart of good decision making. It is incumbent upon all involved in this data sharing ecosystem, that consumers and small and midsize businesses are empowered with the data they need to make the best decisions for themselves, their families, and their organizations.

Thank you again for the opportunity to address the task force and answer any questions you may have.



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

Regarding

“Preserving the Right of Consumers to Access Personal Financial Data”

September 21, 2021

Chi Chi Wu

Staff Attorney

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

7 Winthrop Square, 4th Fl.

Boston, MA 02110

617-542-8010

cwu@nclc.org

Testimony of Chi Chi Wu,
National Consumer Law Center
Before the U.S. House of Representatives Committee on Financial Services
Task Force on Financial Technology
regarding
“Preserving the Right of Consumers to Access Personal Financial Data”
September 21, 2021

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

Introduction

There has been a tremendous amount of interest in the growing use of data from consumers’ bank accounts and other financial accounts to provide a variety of financial products and services, generally facilitated by third parties called “data aggregators.” This topic is the subject of a rulemaking from the Consumer Financial Protection Bureau (CFPB) under Section 1033 of the Dodd-Frank Act,² which requires banks and other financial services providers to make financial account data available to the consumer, subject to CFPB rules. The Section 1033 rulemaking has garnered a significant amount of attention and even a mention in President Biden’s Executive Order on competition.³

We support the call in President Biden’s Executive Order for CFPB to continue the Section 1033 rulemaking. Access to consumers’ financial account data has the potential to enable many products and services that may be beneficial to consumers. At the same time, the intensely detailed and sensitive data inside consumers’ financial accounts can also be used for less beneficial purposes, such as debt collection or targeting consumers for predatory or exploitative products. Data also must be shared in a secure fashion, safe from unauthorized access and data breaches. Whether access to financial account data benefits or harms consumers will depend on whether the CFPB’s 1033 rule, rules by other federal agencies, and any new legislation contain

¹ The National Consumer Law Center is a nonprofit organization specializing in consumer issues on behalf of low-income people. We work with thousands of legal services, government and private attorneys, as well as community groups and organizations, from all states who represent low-income and elderly individuals on consumer issues. *Fair Credit Reporting* (9th ed. 2017) is one of the eighteen practice treatises that NCLC publishes and annually supplements. This testimony was written by Chi Chi Wu, with the assistance and editorial review by Lauren Saunders.

² See CFPB, Consumer Access to Financial Records, 85 Fed. Reg. 71003, 71011 (Nov. 6, 2020).

³ Executive Order on Promoting Competition in the American Economy, July 9, 2021, <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/> (“The Director of the Consumer Financial Protection Bureau, consistent with the pro-competition objectives stated in section 1021 of the Dodd-Frank Act, is encouraged to consider: (i) commencing or continuing a rulemaking under section 1033 of the Dodd-Frank Act to facilitate the portability of consumer financial transaction data so consumers can more easily switch financial institutions and use new, innovative financial products”).

strong consumer protections that ensure the three “C”s and one “D” for access to this valuable source of information:

- Consumer Choice and Control
- Competition
- Consumer Protection
- Data Security

Background: Benefits and Risks of Financial Account Data

Many stakeholders have promoted the benefits of consumer-authorized financial account information for various purposes, including the 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. Our primary focus has been on the use of financial account data for purposes of credit underwriting.

Use of financial account data could benefit the 45 million “credit invisible” consumers who lack a credit history or have files so skimpy that a credit score cannot be generated.⁴ Financial account data could allow credit invisible consumers to obtain affordable credit based on an analysis of the cash flows in the consumers’ bank or prepaid card accounts, *i.e.*, the pattern of debits and credits and balances. Cash flow data has shown significant promise as a form alternative data for underwriting, perhaps the most promising form.⁵ Indeed, the CFPB, along with the other banking regulators, has encouraged the use of cash flow data because of this underwriting potential, cautioning that other types of data could present “greater consumer protection risks.”⁶

There are indications that credit invisible customers of larger banks already have an on-ramp to credit because of cash flow data. It appears that larger banks may be approving credit cards based on deposit account information at their own institutions.⁷ Customers of smaller banks or banks that do not issue credit cards do not have the same benefit. Consumer-authorized data access could level that playing field.

⁴ Kenneth Brevoort, Philipp Grimm & Michelle Kambara, CFPB Office of Research, CFPB Data Point: Credit Invisibles 12 (May 2015), http://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf.

⁵ FinRegLab, The Use of Cash-Flow Data in Underwriting Credit: Empirical Research Findings (July 2019), https://finreglab.org/wp-content/uploads/2019/07/FRL_Research-Report_Final.pdf.

⁶ CFPB, Federal Reserve Board, FDIC, Office of the Comptroller of the Currency, and National Credit Union Administration, *Interagency Statement on the Use of Alternative Data in Credit Underwriting* (December 2019), https://files.consumerfinance.gov/f/documents/cfpb_interagency-statement_alternative-data.pdf.

⁷ Data Point: Becoming Credit Visible, June 2017, https://files.consumerfinance.gov/f/documents/BecomingCreditVisible_Data_Point_Final.pdf, at 33 (noting that “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.”).

In addition to credit underwriting, access to account data could allow consumers to more easily change financial institutions. 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. Consumers should have access to their data to enable comparison shopping and switching providers.

However, access to the financial account data also poses risks to consumers. The intensely detailed and sensitive data inside consumers' accounts can also be used for less beneficial purposes. Some predatory lenders may use the timing and history of inflows and outflows from consumers' accounts to fine tune their ability to collect, but not necessarily the consumers' ability to afford credit while meeting other expenses. Financial account data could even be sold or shared to debt collectors to figure out the best time to collect debts by analyzing when income comes in and can be grabbed.

A consumer's deposit account contains a wealth of information about the consumer's income, where they shop and what they buy, their spending patterns and a variety of other sensitive personal information. Creditors could use this information to make decisions based on where the consumer shops (i.e., dollar stores vs. high-end boutiques) instead of the individual's credit risk.⁸

Financial account data has been touted as a means to promote financial inclusion, and research has found that it holds promise for helping borrowers of color who might otherwise face constraints on their ability to access credit.⁹ However, there still will be disparities by race given the unequal economic positions of households of color and white households, as well as racial disparities in the impact of overdraft practices, as discussed on page 9. When financial account data is fed into algorithms or artificial intelligence models, the results could replicate those disparities.

Whether financial account data ultimately benefits consumers will depend on how vigorous the rights and protections for consumers are. Consumers must have choice and control over our own data; competition must flourish and not be stifled; consumer protections must be strong and forceful; and data security requirements must be robust.

⁸ For example, a professor at U.C. Berkeley's Haas Business School found that "spending on entertainment (such as video, audio, magazines, newspapers, toys and pets) predicts worse credit outcomes. Spending on categories that predict worse consumer credit outcomes tend to also predict smoking and lower education (proxies for impatience), suggesting that impatience is central for consumer credit outcomes." This research could prompt creditors to examine a consumer's purchases in underwriting, leading to lower approvals or higher prices for pet owners or consumers with too many streaming subscriptions. Annette Vissing-Jorgensen, *Consumer Credit: Learning Your Customer's Default Risk from What (S)he Buys*, Aug. 20, 2021, <http://faculty.haas.berkeley.edu/vissing/VissingJorgensenConsumerCredit2021.pdf>

⁹ FinRegLab, *The Use of Cash-Flow Data in Underwriting Credit: Empirical Research Findings* (July 2019), https://finreglab.org/wp-content/uploads/2019/07/FRL_Research-Report_Final.pdf.

Element 1: Consumer Choice and Control

The most important principle for access to financial account data is that it must always be the consumer's choice, and consumers should have full control over their information. *Pro forma* consent is not sufficient; the decision must be an affirmative, knowing, and conscious decision. Consumers should also have the power to shut off the data spigot and to delete the information if they change their mind, as well as the power decide what data elements will be shared.

While data aggregators currently seek consumers' consent, this alone is not sufficient. First, it is unclear whether consent as currently obtained from consumers is truly knowing and voluntary. When consumers click "I agree," many do not understand they are turning over all their deposit account data to a third party. A November 2019 survey by The Clearing House (TCH) found that 80% of financial app users were not aware that apps may use third parties to access consumers' financial information.¹⁰

Even when consumers do truly consent knowingly and voluntarily, they may assume the data will only be used for the immediate purpose for which they authorized accessed. They may not realize the access is not limited to that purpose; that more data may be accessed than is necessary; or that access may not be restricted in time but could continue indefinitely. Access may go on far longer than expected by a consumer who envisioned a one-time or limited access.

Consent may not be truly voluntarily if the consumer is forced to provide it as a condition of obtaining the credit or services, even when account data is not necessary such as when a consumer has a thick credit file with a high credit score. Today, people can easily choose to avoid products that require use of a data aggregator. But as the use of access to financial 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 a potential employer wants to pull a credit report.

Finally, consent is not actually required by any statutory scheme, even the Gramm-Leach-Bliley Act (GLBA), which only provides for an opt-out of sharing. It is competitive forces that compel banks not to share this data, and such forces could shift with a change in the market. Indeed, there is currently a project that would use data from the consumer reporting agency Early Warning Services (EWS) to supply cash flow information for credit invisible consumers via the Big Three credit bureaus (Equifax, Experian, TransUnion). While this project does have benefits for these consumers, consent will not be required for creditors to obtain the EWS data. This lack of consumer control is less preferable to a system where the consumer must give permission to access to their financial account information, as it deprives consumers of the autonomy over their data.

To avoid the risks to consumer control, privacy, and misuse of their data, the following principles must be followed.

¹⁰ Statement of Natalie S. Talpas, PNC Bank, for CFPB Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act, February 26, 2020, https://files.consumerfinance.gov/f/documents/cfpb_talpas-statement_symposium-consumer-access-financial-records.pdf (citing The Clearing House, Consumer Survey: Financial Apps and Data Privacy, November 2019).

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

- 1. Data aggregators and data users should not be allowed to use purported consent to permit uses that consumers do not expect or understand.**
- 2. Use by data aggregators and data users must be limited by purpose.** A consent to use deposit account data for credit underwriting 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:

- 3. Consumers should always have true choice in whether to share their deposit account data as a substitute or supplement for a credit score.** Creditors and other users should not be permitted to require consumers to share bank transaction data if they could have received credit or other services without it.
- 4. Aggregators should not be permitted to share deposit account transaction data for non-financial purposes,** such as employment, insurance, or government licensing or benefits. Needs-based government programs should be entitled to only a snapshot of current balances.
- 5. Consent must be real, knowing, affirmative, and meaningful.** It should never be buried in fine print. It must always be in a separate stand-alone “document,” *i.e.*, webpage or dashboard. The role of the aggregator must be disclosed in a manner that consumers realize it is a separate third-party intermediary that is accessing their account data.

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

- 6. Consent must be limited by data element (i.e., data minimization).** A consumer should be able to control sharing of 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. Not every use case needs all of the information in a consumer’s account, and users should only receive what they need for their application to function properly.
- 7. 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.
- 8. Consumers should have multiple, simple options for ending data sharing and deleting information.** Some banks and data aggregators are developing consumer dashboards where consumers can see who is accessing their data and easily turn it off. Multiple access points – at the bank, at the data aggregator, *and* at the end user app – are necessary.

Element 2: Competition

Consumer-permissioned bank account data could represent a paradigm shift in assessing the creditworthiness of consumers. For decades, consumers and their data have been held captive to abuses and exploitation by the Big Three credit bureaus, *i.e.*, the nationwide consumer reporting

agencies (CRAs). The credit bureaus have created a credit reporting system that has unacceptably high levels of errors as well as a biased and dysfunctional dispute system.¹¹

There is a frequent refrain that the consumer is not the customer of the credit bureaus; instead, our data is their commodity. Our consent is never required to harvest our information and, until the advent of security freezes, we could not even prevent its dissemination. The credit reporting system is an oligopoly of three companies where market forces do not work and consumers have no choice but to be beholden to those companies.

That all has the potential of changing with consumer-authorized data from deposit and financial accounts. This is a source of data that can serve as potential competition to the credit bureaus. It may be more predictive. It could be more accurate than credit bureau data, not only because the source is drawn directly from the consumer's deposit account but because consumers could have more control over it. Consumers must authorize access to the data, and as discussed above, they should have the ability to shut off access whenever they want. If an aggregator does a terrible job with the accuracy of data, the consumer should have the ability to revoke authorization and delete their data from the aggregator's database.

Consumer control would not only help with accuracy as a curative measure, it would help with incentives to ensure accuracy on a prospective basis. If an aggregator knows that too many errors will result in consumers revoking their authorization and deleting their data, the aggregator is likely to take measures to ensure and improve accuracy.

American consumers desperately need to have an alternative to the Big Three credit bureaus. That competition could come from aggregators of consumer-authorized data. Of course, one risk that we are already beginning to see is that the Big Three have started purchasing alternative data providers. For example, Experian purchased Clarity while TransUnion purchased FactorTrust and Equifax purchased Teletrack. All three of the purchased companies are CRAs focused on subprime credit. In other cases, the credit bureaus form partnerships with alternative data providers to access their data. Equifax has a partnership with Yodlee, while Experian has a deal with Finicity, both of which are data aggregators.

While *partnerships* may be understandable, it would be another matter and very troubling if the Big Three creditors actually purchased these and other data aggregators. Anti-trust enforcement of such sales and acquisitions is critical.

Moreover, if bank account data flows through the credit bureaus, even if the initial use is cash flow underwriting, the result could be simply more data in consumer credit reports over which consumers lose control. Simply adding more data to the credit reporting system is less beneficial than having new alternative sources to create competition. And if data gets incorporated into credit reports or is sold and resold, consumers may not even be aware of new uses, let alone have the protection of needing to consent.

¹¹ See NCLC, Automated Injustice Redux: Ten Years after a Key Report, Consumers Are Still Frustrated Trying to Fix Credit Reporting Errors, Feb. 25, 2019, <https://bit.ly/ajustre>.

Element 3: Consumer Protection

It is clear that existing consumer protection laws apply in the context of consumer authorized account data. If used for credit underwriting, the Fair Credit Reporting Act (FCRA) applies and the Equal Credit Opportunity (ECOA) is implicated. The Electronic Funds Transfer Act (EFTA) applies if unpermissioned access to data leads to an unauthorized charge, or if a financial institution using shared data makes a payment or deposit error.

Some stakeholders have claimed that there is regulatory uncertainty as to the applicability of these laws, which they argue impedes innovation.¹² We do not believe that the application of existing laws is either uncertain or a negative circumstance hindering innovation. We have seen many examples over the years of new entrants asserting that well-established statutes do not apply to them because they use novel innovations or technology. They ignore the fact that despite being drafted several decades ago, the federal consumer protections are written broadly, and their core elements generally do not hinge on specific technologies. They are not limited to depository institutions or brick & mortar lenders.

1. Electronic Funds Transfer Act

The most critical principle with respect to EFTA is this one: the use of data aggregators should not deprive consumers of their protection against unauthorized charges or other errors, nor make it more difficult for the consumer to invoke their EFTA rights to correct errors and reverse unauthorized charges. Of the stakeholders in authorized data access, the consumer is least able to bear the cost of a loss. As we all well know, many consumers live paycheck to paycheck, with 40% of Americans who would struggle with an unexpected \$400 bill.¹³ Many consumers cannot afford the unexpected loss that would occur if their EFTA rights were undermined in the fights between financial institutions and data aggregators.

The CFPB recently clarified several questions that have arisen regarding unauthorized transfers that occur as a result of data sharing. The CFPB stated that a transfer is unauthorized within the meaning of Regulation E, and the consumer is protected from liability, even if the consumer was fraudulent induced into sharing account access information or if the consumer was negligent. The CFPB also stated that a financial institution cannot rely on a modification or waiver of

¹² The CFPB reflected back these concerns in its Advanced Notice of Proposed Rulemaking for Section 1033. See CFPB, Consumer Access to Financial Records, 85 Fed. Reg. 71003, 71011 (Nov. 6, 2020). The CFPB also recently clarified several questions arising under the EFTA regarding unauthorized transfers that arise out of data sharing. See CFPB, Electronic Fund Transfers FAQs, <https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/>.

¹³ Federal Reserve Board, Report on the Economic Well-Being of U.S. Households in 2018 - May 2019; Dealing with Unexpected Expenses, <https://www.federalreserve.gov/publications/2019-economic-well-being-of-us-households-in-2018-dealing-with-unexpected-expenses.htm>.

Regulation E liability protections in the account agreement on the basis that the consumer has shared account information with a third party.¹⁴

Consumers also are not in a position to prevent unauthorized charges or other errors that could occur through use of a data aggregator. Nor should they be caught in the middle of a finger pointing exercise between the financial institution, the data aggregator, and the data user. The consumers' right to contest unauthorized charges and to dispute error directly through their financial institution must be respected.

2. Equal Credit Opportunity Act

Data accessed by aggregators, like any other alternative data, must not be used in a fashion that results in discrimination or disparate impacts on consumers in vulnerable communities. Deposit account data will almost certainly exhibit disparities by race. For one thing, a key factor likely to be used by scoring models is overdrafts, and Black consumers are disproportionately affected by bank overdraft practices.¹⁵ **Indeed, the ability of cash flow data to help minority and low-and moderate-income consumers will not bear fruit unless and until bank overdraft abuses are brought to an end.**

As discussed above, deposit accounts can include a host of sensitive information, including what neighborhoods and stores the consumer shops in. Location or geographic neighborhood is one way that creditors have inappropriately assessed creditworthiness by association.¹⁶ The type of store or establishment a consumer frequents may also reflect race or ethnicity.

Thus, use of account data could lead to racial or other disparities not based on the individual's credit risk. 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 research indicates otherwise.¹⁷ Studies and news

¹⁴ See CFPB, Electronic Fund Transfers FAQs, <https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/>.

¹⁵ See Pew Charitable Trusts, Heavy Overdrafters, April 2016, at 7, <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).

¹⁶ Jeffrey S. Morrison & Andy Feltoovich, 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.").

¹⁷ See Elisa Jillson, Federal Trade Commission Aiming for Truth, Fairness, and Equity in Your Company's Use of AI, Apr. 19, 2021, <https://www.ftc.gov/news-events/blogs/business-blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai> ("Advances in artificial intelligence (AI) technology promise to revolutionize our approach to medicine, finance, business operations, media, and more. But research has highlighted how apparently "neutral" technology can produce troubling

reports have shown that computers can discriminate too, from mortgage automated underwriting systems¹⁸ to healthcare delivery.¹⁹

Data that is used for credit purposes – including data obtained through data aggregators – is subject to the ECOA. Data that is using in housing decisions – as 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 or laws against unfair, deceptive, or abusive practices.

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.

3. Fair Credit Reporting Act

One of the contentious issues regarding the role of data aggregators has been coverage under the Fair Credit Reporting Act (FCRA). As those familiar with the FCRA know, the terms “consumer report” and “consumer reporting agency” under the Act are not limited to the Equifax, Experian, and TransUnion. Instead, the terms are broad and expansive, covering entities such as criminal background check vendors, tenant screening agencies, and deposit account screening databases (ChexSystems, EWS). These terms also can apply to new technology companies, including data aggregators that provide third party information used for credit underwriting or other FCRA covered purposes. Indeed, a major data aggregator has also taken the position that aggregators are likely covered as CRAs when their data is used for credit underwriting.²⁰

Despite being 50 years old and the first federal privacy law, the FCRA has withstood the test of time. It was written broadly, based on basic principles of fair information practices:

outcomes – including discrimination by race or other legally protected classes”; discussing various studies documenting AI producing racial disparities).

¹⁸ See Emmanuel Martinez and Lauren Kirchner, The Secret Bias Hidden in Mortgage-Approval Algorithms, The Markup, Aug. 25, 2021, <https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms> (“Holding 17 different factors steady in a complex statistical analysis of more than two million conventional mortgage applications for home purchases, we found that lenders were 40 percent more likely to turn down Latino applicants for loans, 50 percent more likely to deny Asian/Pacific Islander applicants, and 70 percent more likely to deny Native American applicants than similar White applicants. Lenders were 80 percent more likely to reject Black applicants than similar White applicants”).

¹⁹ See Eliane Rössli, Brian Rice, Tina Hernandez-Boussard, Bias at Warp Speed: How AI May Contribute to the Disparities Gap in the Rime of COVID-19, Journal of the American Medical Informatics Association, Vol. 28, Issue 1, January 2021, <https://doi.org/10.1093/jamia/ocaa210> (“In this frenzy, the risk of producing biased prediction models due to unrepresentative datasets and other limitations during model development is higher than ever. If not properly addressed, propagating these biases under the mantle of AI has the potential to exaggerate the health disparities faced by minority populations already bearing the highest disease burden.”).

²⁰ Finicity, FCRA and Data Agents White Paper, Feb. 11, 2001, <https://www.finitycity.com/fcra-data-agents/>.

- *The right to have information be accurate:* The FCRA requires “reasonable procedures for maximum possible accuracy” from consumer reporting agencies.
- *The right to correct errors:* Consumers have the right to dispute inaccurate information and get it corrected.
- *The right to access information about ourselves:* The FCRA gives consumers the right to disclosure of information about themselves in the files of a consumer reporting agency.
- *The right to know when information is used against us:* Consumers get an “adverse action” notice when information in the form of a consumer report is used to deny them credit, employment, insurance, rental housing, or many other financial essentials.
- *Privacy protections to prevent inappropriate dissemination and use:* Only users with a “permissible purpose” can access consumer reports.

The accuracy and error resolution provisions are among the most critical FCRA protections applicable to data aggregation. Although one might assume that information drawn from consumers’ deposit accounts will be accurate, that might not always be the case as errors might arise as the data is processed and passed along, especially with screen scraping. The FCRA requires CRAs to follow reasonable procedures to ensure maximum possible accuracy, 15 U.S.C. § 1681e(b), and when information is not accurate, gives consumers the right to dispute any errors and seek resolution, 15 U.S.C. § 1681i(a). These FCRA rights must be preserved when financial account data is used for credit or other FCRA-covered purposes.

The FCRA also has specific notice requirements, which are intended to ensure transparency when information from a CRA is used. Mostly importantly, Section 615(a) and (h) of the Act, 15 U.S.C. § 1681m(a) and (h), require users of consumer reports to provide adverse action and risk-based pricing notices when information from a CRA has been used to deny them credit or charge them 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.

Finally, if financial account data is a consumer report when it is used for credit underwriting, that same data from the same data aggregator CRA is still a consumer report if used for other purposes.²¹ To the extent that data from an aggregator is never used for an FCRA-covered purpose and is never part of a consumer report, similar fair information rights are necessary, *i.e.*, accuracy, dispute rights, file disclosures, and notices. However, it is critical that any regulation setting up a separate system of rights not undermine FCRA coverage. If there is uncertainty as to whether certain data qualifies as a “consumer report,” any regulation should explicitly provide that nothing in it shall be construed to limit or restrict the applicability of the FCRA. FCRA coverage is preferable because it is a time-proven statute with an established body of law and clear, enforceable consumer rights.

²¹ See National Consumer Law Center, Fair Credit Reporting § 2.2.5.4 (9th ed. 2017), updated at www.nclc.org/library.

4. Data aggregators should be subject to CFPB Supervision

There are a number of areas where data aggregators need more oversight, including data security, privacy, and compliance with consumer reporting and fair lending laws. While the industry is still in its relative infancy, the CFPB has the opportunity to ensure that it benefits consumers and does not cause harm.

Thus, we have advocated that as part of the Section 1033 rulemaking, the CFPB should issue a rule establishing supervisory authority over the larger participants in the data aggregator market. The CFPB has authority over data aggregators as providers of account information,²² as material service providers,²³ or as providers of a product or service that will likely have a material impact on consumers.²⁴ If the data aggregator is a CRA, it may already be a larger participant in the consumer reporting market and should be examined.

Element 4: Data Security

Data security is obviously critical in any system that accesses or uses financial account data. There should be data security obligations on the part of both the aggregator and the end user.

1. Screen Scraping vs APIs

With consumer-authorized data, access is often gained by using the consumers' username and password to access the account (often referred to as "screen scraping"). Screen scraping is less than optimal from a data security perspective; this is one reason we believe the industry should move away from screen scraping.

Many data aggregators have worked to strike agreements with financial institutions to access account data through secure automated programming interfaces (APIs). There appears to be universal support that data aggregation should move away from screening scraping and toward APIs. Consumer groups support efforts to increase the use of APIs and eliminate screen scraping, and consumer groups have been participating in the Financial Data Exchange (FDX).

However, screen scraping should not be prohibited unless and until all consumers at every financial institution have the right and ability to access their own data using more secure means such as an API. A prohibition on screen scraping without such universal access would give banks and other institutions the upper hand and ability to prematurely shut out access.

2. Data Security

Data security is obviously critical in any system that accesses or uses consumers' account data. The main governing law for data security is the Gramm-Leach-Bliley Act (GLBA).

²² 12 U.S.C. § 5481(15)(A)(ix).

²³ 12 U.S.C. § 5481(26).

²⁴ 12 U.S.C. § 5481(15)(A)(x).

In terms of regulatory regimes, CRAs are subject to the Federal Trade Commission's Safeguards Rule, and data aggregators are likely subject to that rule as well. The FTC Safeguards Rule is currently the subject of a rulemaking to strengthen its requirements.²⁵ Congress should urge the FTC to complete this rulemaking to improve data security for CRAs, data aggregators, and other non-bank entities.

However, even with enhanced protections, the Safeguard Rule and FTC's authority over data security are missing a critical element – supervision, which the FTC has neither the authority nor the infrastructure to conduct. As discussed above, the CFPB could supervise data aggregators, and already supervises larger participant CRAs - but GLBA specifically excludes the CFPB from jurisdiction over its data security provisions.²⁶ Since the Equifax data breach in 2017,²⁷ we have urged Congress to transfer the GLBA data security authority to the CFPB for CRAs, and we would urge the same with respect to data aggregators.

* * * * *

Financial account information holds great promise but also great risk. It could open the doors to credit for millions of underserved Americans, including consumers of color, as well as help facilitate competition. It could also result in products and innovations that benefit consumers and enable portability of financial accounts.

There is a dark side to the sharing of account data, though. It could also lead to unwanted wider and wider access to consumers' private data. The nightmare scenario is a system where every consumer - thin or thick file, high FICO score or not - must automatically give up the privacy of their bank account information and allow each creditor, employer, landlord, insurer, and government agency a direct and permanent digital pipeline to their bank account data. It is up to the regulators, and ultimately Congress, to make sure that this data promotes consumer welfare without harming our best interests.

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

Supplemental materials

(1) NCLC, etc. Comments to the CFPB in Response to the ANPR Regarding Consumer Access to Financial Records Under Section 1033 of the Dodd-Frank Act, Feb. 4, 2021, https://www.ncle.org/images/pdf/credit_reports/Comments_CFPB_1033_ANPR.pdf.

²⁵ 84 Fed. Reg. 13158 (Apr. 4, 2019).

²⁶ See 15 U.S.C. §§ 6801(b), 6805(b)(1). The CFPB could and may already be supervising the CRAs for data security under other authority, such as the prohibition against unfair, abusive or deceptive practices under Section 1031 of the Consumer Financial Protection Act.

²⁷ Testimony of Chi Chi Wu before the U.S. House of Representatives, Committee on Financial Services, regarding Examining the Equifax Data Breach (Oct. 25, 2017), https://www.ncle.org/images/pdf/credit_reports/ncle-tstmny-hfsc-equifax-hearing-102517.pdf.

(2) NCLC Written Statement for CFPB's Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act, February 12, 2020, https://files.consumerfinance.gov/f/documents/cfpb_wu-statement_symposium-consumer-access-financial-records.pdf

(3) 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, <https://www.nclc.org/images/pdf/cons-protection/testimony-lauren-saunders-data-aggregator-nov2019.pdf>

(4) NCLC Comments in Response to Requests for Information: Consumer Access to Financial Records, Docket No. CFPB-2016-0048, Feb. 2017, <https://www.nclc.org/images/pdf/rulemaking/comments-response-data-aggregator.pdf>



**United States House of Representatives Committee on Financial Services
Task Force on Financial Technology**

**Preserving the Right of Consumers to Access Personal Financial Data
Tuesday September 21, 2021**

Testimony of Manning Field, Chief Business Officer, Acorns

Introduction

Chairman Lynch, Ranking Member Davidson, Chairwoman Waters, Ranking Member McHenry and members of the Task Force, I applaud you for holding this important hearing and thank you for providing me the opportunity to submit this written testimony. The complexities facing policymakers around the issues of consumer data are significant, but the issue itself is quite simple: customers own their data and they need a portable and secure way to access their data.

Background on Acorns

Acorns was founded on the premise that it is too difficult and complicated for everyday consumers to start saving and investing for their future. We are committed to protecting economically vulnerable consumers, with the hopes of inspiring them to shape their future by investing in themselves for the long-term.

Launched in 2014, Acorns pioneered micro-investing, enabling customers to easily and automatically invest in diversified portfolios that are tailored to the risk and return goals of that customer. Through our innovations and unwavering commitment to introduce products that serve the best interest of the customer, we have helped ten million Americans save and invest nearly 10 billion dollars; 60% of those customers are first time investors.

Consumer Data and Acorns

Acorns' solution to helping investors save for their futures would not be possible without customers' willingness to share their financial data in a machine readable format. Our business model rounds up customers' everyday spending and invests that spare change in a diversified investment portfolio. Logistically, that means Acorns connects to our customers' debit and credit card accounts -- with their explicit consent -- to help customers invest in as seamless a way as possible. We partner with the financial institutions our customers' use to "round up" on transactions. As such, Acorns has a unique perspective in the consumer data ecosystem as our technology is active with over 10,000 banks and credit unions.

As the fintech and traditional financial institutions have wrestled with this topic, we have come to an imperfect private solution. Acorns welcomes the committee's attention on this issue and believes there is a role for the government to play in ensuring consumers have access to their own data. Structuring that data will help consumers and innovators by creating a clear, executable way to manage and share information.

As the Task Force on Financial Technology and broader Financial Services Committee think through the issues of consumer data, we urge you to consider the following topics:

The importance of standardization

In the current environment, a lack of standardization has resulted in an imperfect private solution. Data and access are not standardized, and neither are security and reliability. This lack of uniformity makes it difficult to separate good actors from bad. We believe that regulation is vital to create the necessary standardization to foster further innovation and protect consumers in this space.

Every institution's data is different, both in structure and how it is labeled, creating challenges for sharing. Standardization will provide customers peace of mind that their data is secure and that the institutions they do business with are all complying with the same regulatory regime.

Standardization will also ease the burden of compliance for financial institutions, both traditional industry stakeholders and new entrants, by mapping out the "rules of the road" so that all participants know what is required.

Standardization should extend to access and security. Access to consumer data should be the same for all market participants - and all those market participants should be held to the same security standards. Consumer banks should not dictate what innovative products are available, nor should an innovative product expose a consumer to a higher risk of security breach than a traditional bank.

Finally, standardization will lead to faster innovation and lower cost - aiding consumers, expanding access to unserved populations while helping all market participants.

Service level standards on the stability of the data connections

Any institutions that make their data available should be subject to service level standards so that consumers are not at a disadvantage. The Task Force should weigh how the CFPB can best ensure that all market participants are held to an industry standard for data connectivity to guard against consumers being prevented from freely choosing financial services products and providers.

A shared commitment to remediate issues where customers are negatively impacted due to a poor connection

While considering how best to implement an industry wide service level standard, enforcement will be key. Specifically, if an industry participant is unable to meet their data connectivity

commitment, they should face consequences for not maintaining their services. Appropriate enforcement mechanisms should be identified to protect both consumers and market participants negatively impacted by other market participants' unreliable connection. This reliability standard should apply equally to institutions, fintechs and intermediary third-party data providers.

A qualification standard that needs to be established and renewed annually for all participants

To de-risk aspects of the industry, the minimum qualification standards should be established for all market participants. This certification could help prevent participants who are poorly capitalized, who have insufficient security practices from taking part in this ecosystem, or who do not use the data in a way that supports the financial best interests of the consumer.

Policymakers should contemplate the creation of a mechanism with qualifications regarding certification in a way that allows for updates on a regular basis (annually) to have an opportunity to adapt as technology develops and as security threats evolve.

Impact on community banks and credit unions

We also recognize that some of these suggestions might be overly burdensome for community banks and credit unions. Acorns is aligned with these institutions with respect to how we approach customers, and we suggest an appropriate exemption for community banks and credit unions under a certain size.

Conclusion

Rather than view these challenges as divisive - we hope Congress and the CFPB embrace this opportunity to foster greater collaboration between financial institutions and to protect consumers. Innovation will always create new entrants, but startup fintechs should be additive to the traditional financial institutions long-entrenched in this space. While weighing the various consumer data factors, we hope policymakers focus on creating a necessary balance to protect consumers in a way that reflects the realities of the modern financial landscape: traditional financial institutions are an important part of consumers' economic well being, and innovative new entrants can help bridge the gap for Americans who are being left behind in today's economy.

When we get to the heart of what we are trying to accomplish, we are not accounts or data connections; we are people and communities. Implementing Dodd-Frank Section 1033 has the ability to level the playing field for Americans and we are proud to contribute in a way that supports our economy and our society, so that everyone has the opportunity to pursue their version of the American dream.



September 27, 2021

The Honorable Stephen Lynch
Chair
Task Force on Financial Technology
House Financial Services Committee
2109 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Warren Davidson
Ranking Member
Task Force on Financial Technology
House Financial Services Committee
2113 Rayburn House Office Building
Washington, D.C. 20515

Dear Chair Lynch and Ranking Member Davidson:

Akoya¹ appreciates the opportunity to provide its perspectives on the important topic of consumer access to personal financial data. Akoya believes that the benefits of consumer data access, which has been a key driver of innovation in the financial services industry, will be enhanced if such access is provided in a safe, secure, and transparent manner. Accordingly, Akoya's mission is to transform the way consumers provide access to their data.

Akoya believes that consumer data access will be enhanced if the following four practices are adopted. *First*, the industry must move away from screen scraping to safer technologies, thus eliminating the need for consumers to share their login credentials with a third party in order to authorize sharing of financial data. *Second*, financial institutions should empower consumers to have more control over their data by (i) requiring clear, conspicuous consent from consumers to permit third party access to consumer data, (ii) helping consumers monitor access to their data on an ongoing basis, and (iii) providing a means for consumers to revoke access to their data at any time. *Third*, data users and data aggregators should obtain explicit and informed consent from consumers in order to access their data and should only access data that are strictly necessary to the service they are providing. *Fourth*, if data access results in harm, such as through data loss, compromise, misuse, or other security-related incident, the party that causes the harm should bear the liability and be held responsible for the risks their activities introduce.

The Industry Must Rapidly Move Away from Screen Scraping

Screen scraping has been the primary method for accessing consumer financial data for the last two decades and continues to drive data access today. While there are variations, this process usually involves consumers sharing their login credentials (typically usernames and passwords) used to access their account information on the website of their financial institution with a third party (the "data user") who then, either on its own or by hiring a data aggregator, accesses and retrieves the consumer's financial data on the consumer's behalf. Unfortunately, screen scraping is neither secure nor transparent for consumers.

¹ Originally created within Fidelity Investments, Akoya was developed to eliminate the risks associated with screen scraping. In February 2020, realizing the value Akoya brought to the entire financial services industry, The Clearing House and 11 of its member banks (Bank of America, Capital One, Citi, Huntington Bank, JPMorgan Chase, KeyBank, PNC Bank, TD Bank, Truist, U.S. Bank, and Wells Fargo) became equal owners of the now independent company alongside FMR LLC (the parent company of Fidelity Investments).

Often, consumers do not understand the scope or duration of access they are providing to data users and data aggregators. In fact, many consumers are unaware that their login information and financial data are stored by the data aggregator instead of, or in addition to, the data user. Data aggregators also often access more data than the data user needs to provide the service the consumer wants. Moreover, data aggregators may continue to access consumer data even when a consumer no longer uses the service provided by the data user because there is not a clear and simple process for consumers to revoke the aggregators' ongoing access to their data without having to change their login credentials at their financial institution. This can result in third parties holding consumer login credentials and continuing to access a consumer's financial data for an indefinite period, which poses a significant privacy risk.

There are also significant security risks with screen scraping, as many consumers use the same login credentials across multiple web services.² This leaves consumers' accounts vulnerable to "credential stuffing" – a type of cyberattack where bad actors obtain stolen consumer login credentials and use them repeatedly across several sites until they find a match. In a September 2020 notification, the Federal Bureau of Investigation (FBI) highlighted that "[c]redential stuffing attacks accounted for the greatest volume of security incidents in the financial sector at 41 percent of total incidents from 2017 through 2019, according to a 2020 cybersecurity firm report."³

The FBI notification also stated the "increasing prevalence of credential stuffing attacks since 2017 correlates with an increase in leaked credentials available on the dark web, which are expected to number in the billions, according to a 2020 cybersecurity firm report and open-source reporting."⁴ In fact, a report from McAfee and the Center for Strategic and International Studies (CSIS) found that there are more than 15 billion stolen consumer login credentials for sale on the dark web.⁵ The Securities and Exchange Commission (SEC) also published an alert in September 2020 entitled "Cybersecurity: Safeguarding Client Accounts against Credential Compromise," which focused on "'credential stuffing' — a method of cyber-attack to client accounts that uses compromised client login credentials, resulting in the possible loss of

² Recently, "[a] Google survey found that at least [65% of people](#) reuse passwords across multiple, if not all, sites; [a]nother recent survey found that [91% of respondents](#) claim to understand the risks of reusing passwords across multiple accounts, but 59% admitted to doing it anyway; Microsoft recently announced that a staggering [44 million accounts](#) were vulnerable to account takeover due to compromised or stolen passwords; [t]he average person reuses each password as [many as 14 times](#); [72% of individuals](#) reuse passwords in their personal life while nearly half (49%) of employees simply change or add a digit or character to their password when updating their company password every 90 days. These [forced resets](#) are an ineffective tactic; [a]nd it is not just personal accounts. [73% of users](#) duplicate their passwords in both their personal and work accounts; Security.org found that [76% of millennials](#) recycle their passwords; [t]his is why compromised passwords are responsible for [81% of hacking-related breaches](#), according to the Verizon Data Breach Investigations Report." Kim Jacobson, *8 Scary Statistics about the Password Reuse Problem*, <https://securityboulevard.com/2020/04/8-scary-statistics-about-the-password-reuse-problem>.

³ FBI Cyber Division, *Private Industry Notification – Cyber Actors Conduct Credential Stuffing Attacks Against US Financial Sector* (Sept. 10, 2020), <https://www.documentcloud.org/documents/7208239-FBI-PIN-on-credential-stuffing-attacks.html>.

⁴ *Id.*

⁵ Zhanna Malekos Smith and Eugenia Lostri, *The Hidden Costs of Cybercrime*, <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf>.

customer assets and unauthorized disclosure of sensitive personal information.”⁶ Given the risks associated with stolen consumer credentials, it is not surprising that a 2018 report from the United States Department of the Treasury found that “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.”⁷

Fortunately, given technological advances such as application programming interfaces (APIs), it is no longer necessary to rely on screen scraping. APIs act as software intermediaries that allow applications to communicate with one another – and in this case, provide access to data. API-based data access can be used to authenticate and authorize consumers directly with their data holder, thus eliminating the need for login credentials to be held and stored externally by a data aggregator or data user. This significantly mitigates the privacy and security risks stemming from screen scraping. In addition to being more secure, APIs can also enable increased transparency and control for consumers.

Financial Institutions Should Require Clear, Conspicuous Consent from Consumers to Share Data, Enable Consumers to Monitor Access on an Ongoing Basis, and Provide a Means for Consumers to Revoke Access at Any Time

Many consumers neither understand the full scope of access they are providing nor the parties to whom they are providing access. Consumers are often unaware that their login credentials and financial data are stored not only by the data user, but also by data aggregators. Moreover, when consumers no longer use the services of the data user, there is not a clear and simple process for consumers to revoke the authorized parties’ ongoing access to the data without having to change their login credentials at their financial institution. When they cease using the data user’s application, most consumers reasonably assume that access to their data is cut off. Consumers generally are unaware that third parties hold their login credentials and can continue to access their financial data for an indefinite period – a huge privacy risk.

Accordingly, to protect and empower consumers, financial institutions should require clear, conspicuous consent from consumers in order to permit third party access to their data. Financial institutions should also clearly communicate to consumers what type of data is being accessed and by whom and provide a mechanism for the consumer to easily monitor and revoke such access on an ongoing basis. Furthermore, financial institutions should be allowed to periodically ask consumers to reauthorize their consent to ensure that the consumers continue to desire providing authorized data access to their financial data – particularly when sharing sensitive transaction or account information.

⁶ SEC OCIE Risk Alert, *Cybersecurity: Safeguarding Client Accounts against Credential Compromise* (Sept. 15, 2020), <https://www.sec.gov/files/Risk%20Alert%20-%20Credential%20Compromise.pdf>.

⁷ U.S. Department of the Treasury, *A Financial System That Creates Economic Opportunities – Nonbank Financials, Fintech, and Innovation* (July 2018), <https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf>.

The Honorable Stephen Lynch
The Honorable Warren Davidson

- 4 -

September 27, 2021

Data Users and Data Aggregators Should Obtain Explicit and Informed Consent from Consumers in Order to Access Their Data and Should Only Access Data that Are Necessary to the Service They Are Providing

Consumers are typically seeking to use the applications of data users and are permitting access to their data for that purpose. They generally are not intentionally providing access for other purposes. Accordingly, data users and data aggregators should obtain explicit and informed consent from consumers, through consumers' data holders, in order to access their data, and should limit data aggregators and data users' access only to data that are necessary to the service they are providing the consumer. If it wants to access additional data, then the authorized entity should have to obtain specific consumer consent for that additional data. Terms and conditions presented in multi-page documents to consumers should not include open-ended language stating that consumer financial data can be used for "any legal purpose," "for any purpose including..." or other similar disclaimers.

The Party that Causes the Harm Should Bear the Liability

Given the critical role that consumer data access plays in promoting innovation in the financial services industry, data holders, data users, and data aggregators are diligently working together to make progress on technical standards for authorized data access. However, agreements regarding liability have been very challenging to navigate due to the time-consuming and expensive process of negotiating them on a bi-lateral basis. Accordingly, only a small number of industry participants have entered into data-access agreements. Without a coherent liability framework, and in the absence of other agreements, industry participants are incentivized to force consumers to sign away liability in contractual terms and conditions, leaving the financial institution to shoulder all of the burden to aid consumers who are harmed when their data is compromised.

Akoya believes the appropriate liability framework for consumer data access should be based on the principle that the entity that causes the harm, such as through data loss, compromise, misuse, or other security-related incident, should bear the liability and be held responsible for the risks their activities introduce. If there were clarity regarding such a liability framework, competition and innovation would be enhanced as participants throughout the consumer data access ecosystem would have an incentive to improve their security in order to prevent harm from being done to them or their customers.

* * * * *

Akoya appreciates the opportunity to provide its perspective on these important issues. Should you have any questions or need additional information, please do not hesitate to contact us.

Sincerely,

Stuart Rubinstein
Chief Executive Officer

September 2021

Statement for the Record

On Behalf of the

American Bankers Association

Before the

Task Force on Financial Technology

Of the

Financial Services Committee

September 21, 2021

Statement for the Record
On Behalf of the
American Bankers Association
Before the
Task Force on Financial Technology
Of the
House Financial Services Committee

September 21, 2021

Chairman Lynch and Ranking Member Davidson, thank you for the opportunity to submit this statement for the record for the hearing titled “Preserving the Right of Consumers to Access Personal Financial Data.”

The topic of today’s hearing is a timely one that is getting increasing attention. As consumers access novel financial services offerings, it is critical to ensure they retain the protections they have come to expect from their bank. The American Bankers Association (ABA)¹ and our members are working hard to ensure that consumers remain protected when they choose to share their financial data.

Technology has facilitated the creation of a tremendous amount of consumer financial data. The unprecedented proliferation and availability of this data have 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 highlight the timeliness of this issue and the need to ensure that financial data are handled appropriately and securely.

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 competition and 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.

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

We believe that if handled appropriately, access to these data can benefit consumers. **This is why ABA and our members fully support their customers’ ability to access and share their financial data in a secure, transparent manner that gives them control.** Today, banks and technology companies are collaborating to build tools that facilitate access to financial data in a way that protects and empowers consumers.

However, sharing financial information is not without risks. Consumer financial data are extremely sensitive and must be protected appropriately. Accordingly, Congress has recognized the sensitivity

¹ The American Bankers Association is the voice of the nation’s \$22.8 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard nearly \$19 trillion in deposits and extend \$11 trillion in loans. Learn more at www.aba.com.

of financial information and has provided protections for it under the Gramm-Leach Bliley Act of 1999 (GLBA), which creates a legal framework for protecting consumer data, and for sharing that data with third parties. 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.

Consumers understand the importance of protecting their financial data and are skeptical about the safety of their data when shared outside of the bank. This was highlighted by recent data from a Morning Consult survey that showed “U.S. Adults Among the Most Concerned With Data-Sharing Fraud.” In the survey 63% of respondents believed that more sharing of data between financial services companies will lead to more fraud. [16% disagreed] The survey also highlighted privacy concerns, with 48% of respondents reporting that they are unwilling to “share their financial information with a provider that I do not currently use if it meant they would offer me a personalized financial management services.” [34% were willing]²

There is significant work underway to ensure that consumers can share their financial data while maintaining these critical protections. In 2017, under then Director Richard Cordray, the Consumer Financial Protection Bureau (CFPB) released a set of guiding principles that has served as the bedrock for industry collaboration. Since then banks, data aggregators, and other technology companies have worked together to invest in technologies that move away from less secure methods of data sharing like screen scraping to more secure Application Programming Interfaces (API) based standards that give consumers transparency and control when they share their financial data.

This work has been highlighted recently by the Executive Order on Promoting Competition in the American Economy³, and is currently on the CFPB’s rule-making agenda for April 2022.⁴ As the CFPB considers next steps to encourage the development of a data ecosystem that protects consumers, we believe it should focus on supporting market developments that are already well underway. Overly prescriptive standards risk undermining the progress that has been made and if not well crafted, may leave consumers exposed. While we believe that continued industry collaboration is the best way to accomplish our shared goal, there are several regulatory clarifications and other recommendations that would help facilitate the continued development of a responsible data sharing ecosystem.

Given the critical role of the CFPB in this process, the remainder of our statement will make the following recommendations for the CFPB as it looks to encourage the development of this important market consistent with the rights outlined in Section 1033 of the Dodd Frank Act.

- Banks support consumers’ right to share their data as outlined by the CFPB’s principles;
- The industry has made tremendous progress since the CFPB released its principles;
- Prescriptive frameworks would be counterproductive to implementing Section 1033; and

² <https://morningconsult.com/2021/09/07/open-banking-awareness/>

³ <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/>

⁴ <https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202104&RIN=3170-AA78>

- There are areas where the CFPB can provide clarity to allow the market to continue to develop.

Banks support consumers' right to share their data as outlined by the CFPB's principles.

Technology is changing the way consumers engage with their finances and rapidly changing what consumers expect of their bank. Banks are responding to these market changes by investing in new technologies and partnering with startups to bring their customers the latest innovations. These technologies put the branch into consumers' pockets and make it easier to manage their finances. Today, customers expect to be able to access these services across the various platforms they use and to be able to share their data to access new financial services offerings. They also expect to remain protected wherever they receive their financial services. As a result, banks see the ability to allow consumers to securely share their financial data as critical to their competitiveness.

This is why banks have long supported⁵ their customers' ability to share their financial data. However, making this data available is not as easy as flipping a switch. Banks are trusted custodians of their customers' most sensitive data and consumers expect the application of appropriate protections designed to maintain the safety and security of that information wherever they engage with their finances. We believe access to data is only part of the equation that must be supported by robust consumer protections to ensure it benefits, not harms, consumers.

The complexity of this issue and the importance of ensuring that consumers remain protected is why Congress gave the CFPB authority to prescribe standards to implement the rights outlined in Section 1033.

In 2017, the CFPB released a set of principles⁶ to support responsible sharing of consumer data. According to then Director Richard Cordray, "these principles express our vision for realizing an innovative market that gives consumers protection and value." Importantly, these principles recognized the critical balance of ensuring consumers have the ability to share their data, while ensuring they remain protected when they do so.

These principles have served as a flexible bedrock for meaningful industry discussions that has facilitated real progress. Since the principles were released, industry collaboration has led to the development of technical standards, industry utilities, and other technologies and practices that can help enable responsible sharing.

ABA supports these principles which are consistent with our own long-held principles outlining what consumers should expect when they share their financial data.

1. Access

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

⁵ <https://www.consumerfinancemonitor.com/wp-content/uploads/sites/14/2017/02/ABA-Comment-CFPB-Data-Aggregators.pdf>

⁶ https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf

2.Security

Consumers deserve the same level of data security and protection afforded by regulated financial institutions (“bank-level”) regardless of where and with whom they choose to share their data. This means that consumer data are treated the same – and subject to GLBA or substantively similar protections – whether at a bank or a third party.

3.Transparency

Consumers must have transparency about how companies use their financial data, including companies that they permit to access their data. It should be clear to consumers what data a technology company is accessing, which downstream parties are getting access to the data, how long the company is holding this data, and how the data is or may be used. This should be accomplished by affirmative consent and clear, accessible, and understandable legal disclaimers.

4.Control

When consumers share their financial data they should have control over what information is shared, how it is used, and for how long it may be 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 to provide the service. Limiting sharing to necessary data helps minimize privacy risks and allows consumers to clearly 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. Where possible, aggregators should obtain sensitive personally identifiable data directly from the consumer.

The industry has made tremendous progress since the CFPB released its principles.

ABA believes that collaboration among banks, technology companies, and data aggregators is the best way to promote an ecosystem that facilitates responsible data sharing. Since the CFPB released its principles in 2017, industry collaboration has led to tremendous progress that highlights the efficacy of this approach.

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.

Because of the strong progress that has been made in each of these areas, consumers are better protected when they share their financial data today.

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. 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” report⁷.

This is an area where industry has made significant progress. In the fall of 2018 banks, aggregators, and technology companies came together to establish 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 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 member banks, technology companies, and aggregators.

The nature of innovation means that things are constantly changing, and no single technology will always be the right tool to facilitate secure data transmission. Moreover, flexibility is needed to accommodate the wide range of technologies banks currently employ. Prescriptive standards may prevent the most innovative companies from finding new, more secure methods of facilitating data sharing. There are also many different APIs for different solutions and while APIs are the best technology today, banks 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.

Contracts

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

With legacy practices like “screen scraping” the bank has no direct relationship with an aggregator. This is because from a bank’s perspective, an aggregator looks like its customer. Aggregators 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.

This is another area where the industry has made significant progress. Akoya is a network utility that makes it easier for banks and fintech apps to integrate API solutions. Akoya facilitates API connections by providing technical, legal, and security standards among financial institutions, data aggregators, and fintechs. This means that rather than having to create individual relationships with every aggregator or fintech, banks and fintechs can simply join the network and agree to a common set of rules designed to protect consumers. ABA recently hosted a podcast with Akoya and Jack

⁷ <https://www.aba.com/news-research/research-analysis/understanding-apis>

Henry to discuss efforts developments that ensure community banks can offer their customers these products.⁸

Regulation also plays an important role here. Consistent regulation and proactive supervision of data recipients would make it easier for data holders to enter into contracts. Absent this supervision, banks feel the need to secure appropriate protections for their customers through these contracts. If there were a more consistent regulation, data holders would have a degree of confidence that recipients were being examined for compliance with key consumer protection laws, simplifying the contracting process.

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 consumers have consented to share their financial data and provide a transparent portal that allows them to understand what data are shared, limit the data that are shared, and revoke access altogether. These systems can also help trace where data travels and provide visibility on the downstream parties that can access it.

We have seen many large banks unveil permissioning platforms. Wells Fargo's "Control Tower" and JPMorgan Chase's "Security Center" are just a few examples. Core integrations with Akoya offer community banks the ability to offer similar features.

Prescriptive frameworks would be counterproductive to implementing Section 1033.

Today, millions of consumers already have the ability to share their financial information via secure API. This progress has been driven by industry collaboration that is supported by the principles-based approach that the CFPB has taken to date. A more prescriptive approach is not only unnecessary but may undermine the progress that has already taken place and risks leaving consumers exposed if undertaken too narrowly.

In the advanced notice of proposed rulemaking issued in 2020, the CFPB considered whether it should prescribe criteria that identify the specific data fields that should be subject to the access rights described in Section 1033. This would represent a major shift away from the CFPB's current principles-based approach developed under Director Cordray that would likely have serious unintended consequences.

Implementation of prescriptive standards would quickly undermine the progress that has taken place since the CFPB published its principles in 2017. If the CFPB were to announce a new approach to data aggregation, industry participants would pause and quickly step away from existing initiatives that already give consumers more secure methods to share their data.

Prescriptive standards also rarely facilitate innovation. By their very nature, standards are relatively static. In a market that is evolving as quickly as financial services, the data fields that are identified as

⁸ <https://www.aba.com/news-research/podcasts/empowering-community-banks-with-open-finance>

important for today's use cases of aggregated data are unlikely to be appropriate for the innovations of tomorrow.

Prescriptive action cannot focus solely on access but must also address the risks to consumers.

In addition to being unnecessary, prescriptive rulemaking may also put consumers at risk. Any prescriptive rule cannot only focus on defining the data fields, but must also build a robust framework for consumer protection that includes supervision, liability, and data security.

Access cannot be divorced from the other important principles already outlined by the CFPB and must be paired with security, transparency, control, and minimization. Consumers only benefit from access when the financial data retains bank-level legal protections, regardless of the entity that holds the data, and consumer trust in the financial system is maintained. Any effort to prescribe access without also prescribing the protections that must apply to that data would inevitably leave consumers exposed. For example, open banking laws enacted in Europe were only possible because strong general privacy laws already applied to all firms.

Moreover, any action to define the specific data fields subject to Section 1033 would undermine the CFPB's core principle of minimization. All fields included in this definition would inevitably be shared in every instance, rather than only shared if needed for the service a consumer authorized.

Today, many of these protections are implemented through the contracts that govern access. These contracts are either negotiated on a bilateral basis or via industry utilities like Akoya. These negotiations ensure that the right data fields are made available while minimizing the unnecessary data shared and securing protections for consumers.

Any prescriptive action by the CFPB to define the terms of access would also need to address the following critical issues:

- **Supervision:** The CFPB would need to establish a framework for direct supervision of all data recipients including downstream users of financial data to ensure that data are being afforded the appropriate protections.
- **Liability:** The CFPB would need to establish a liability framework that ensures that consumers are made whole in the event of a loss. It is critical that liability sits with the party best able to control for the risk and flows with the data to the entity that the consumer has permissioned to access the data. Any such framework should provide a practical, efficient, and fair means to assign and enforce the liability.
- **Data Protection and Privacy:** The CFPB would need ensure that data privacy requirements are consistent across banks and nonbanks. The FTC Safeguards Rule⁹ (which applies to nonbanks) only sets out the standards and stops short of the important requirements adopted by the federal banking agencies for institutions to (a) establish and maintain appropriate safeguards to ensure the security of the data to which they have access and (b) notify customers as quickly as appropriate after a breach or data loss to allow customers to take steps to protect themselves in the event their information may have been compromised.¹⁰

⁹ 16 C.F.R. 314

¹⁰ For more analysis on the importance of GLBA please see pages 4-5 of ABA's 2017 comments.

<https://www.consumerfinancemonitor.com/wp-content/uploads/sites/14/2017/02/ABA-Comment-CFPB-Data-Aggregators.pdf>

Congress should urge the CFPB to provide clarity to allow the market to continue to develop.

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. Many of these topics are likely to be covered by the upcoming CFPB rulemaking. We believe that Congress should urge the CFPB to consider the following recommendations to ensure that customers of all banks – regardless of their asset size – can control their financial data and fully benefit from financial innovation.

Congress should urge the CFPB to clarify that GLBA applies to financial data throughout its lifecycle.

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, 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.”

Consumers expect that their financial data are adequately protected whether 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 aggregation should be treated as a data processing activity that is financial in nature such that data aggregators fall under the GLBA’s definition of “financial institution” and be subject to all the rules that apply to all other financial institutions. This ensures that data protections apply consistently and continually regardless of where the data originated, where they are transferred, or the type of company 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 Bank Holding Company Act of 1956, Section 4(k).]” This definition includes not only banks, but as interpreted by the Board of Governors of the Federal Reserve, 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 the CFPB should 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.

Congress should urge the CFPB to 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 log-in 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 and shared. In most cases consumers do not have a direct relationship with these companies and must trust that their data are 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 importantly, 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 CFPB. 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, the CFPB should expeditiously initiate 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 CFPB has imposed supervisory authority over the larger data aggregators, it will be better able to monitor – and react to – risks to consumers in this rapidly evolving marketplace.

Congress should urge the CFPB to clarify that data aggregators are subject to Regulation E as service providers.

Under Section 1005.14 of Regulation E, a person that provides an electronic fund transfer service to a consumer but does not hold the consumer’s account is generally subject to Regulation E, (with certain modifications) as a service provider, 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.

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 should be treated as “service providers” under Regulation E, as they enable the use of “access devices” that initiate electronic fund transfers to and from the account. As service providers, they are liable for unauthorized transactions under Regulation E and are subject to 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 commercial or other relationship with the data aggregator, no knowledge of, and no power over the data aggregator’s security system, or any relationship with the aggregator’s end clients. 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 service provider responsibilities of Regulation E support classifying data aggregators as service providers. These include requirements related to error resolution, disclosures, the prohibition against the issuance of unsolicited access devices, and changes in terms notices.

To avoid any ambiguity, the CFPB should confirm in Regulation E or the Official Commentary that data aggregators providing electronic fund transfer services are service providers under Regulation E. Equally important is that data aggregators be examined for their compliance with these consumer protection rules.

Congress should urge the CFPB to require that data aggregators periodically reconfirm consumer authorization to access their accounts.

When consumers authorize a third party to access their financial data, they expect that data sharing is limited to the data needed to provide the service they have authorized. This applies not only to the scope of data being shared, but to the period of time over which that access is granted. Some use-cases of data aggregation are ongoing. However many are one-time events like account ownership verification. Yet, data holders have the ability to store login credentials indefinitely, sometimes continuing to access data years after the consumer has stopped using the service.

Federal Reserve Board Governor Lael Brainard explains this in a 2017 speech:

In examining the terms and conditions for a number of fintech apps, it appears that consumers are rarely provided information explaining how they can terminate the collection and storage of their data. For instance, when a consumer deletes a fintech app from his or her phone, it is not clear this would guarantee that a data aggregator would delete the consumer's bank login and password, nor discontinue accessing transaction information. If a consumer severs the data access, for instance by changing banks or bank account passwords, it is also not clear how he or she can instruct the data aggregator to delete the information that has already been collected. Given that data aggregators often don't have consumer interfaces, consumers may be left to find an email address for the data aggregator, send in a deletion request, and hope for the best.¹¹

We believe that the CFPB should require data aggregators to re-obtain a consumer's consent on a periodic basis to ensure that consumer data are not shared indefinitely.

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

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 the data 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. The bank customers have directed their bank to share their data; a bank's contract simply lays out the terms for how that data are shared and provides a more secure portal for doing so. Such a

¹¹ <https://www.federalreserve.gov/newsevents/speech/brainard20171116a.htm>

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

Banks should not be considered furnishers for purposes of FCRA

Congress should urge the CFPB to make clear that when a bank or other data holder is compelled to share information with a third party at the direction of a customer, the bank and other data holders are not considered to be furnishers for purposes of the Fair Credit Reporting Act (FCRA), regardless of how the third party uses the information. In these cases, banks are merely accommodating the customer and acting as the customer's agent. They are providing information just as they do, for example, when they send bank statements (by paper or electronically) directly to a lender processing their customer's loan application. The only difference is that the information is shared more efficiently using a process that is more convenient for the customer.

In these cases, the customer's agreement to share data is with the data aggregator, not the bank or other data holder. The banks and other data holders have no choice but to share the information and derive no direct or indirect benefit in sharing it. Its agreement with the third party is simply to provide a means for mitigating risk when sharing sensitive information at the customer's direction. In many cases, they may not and often do not know the purposes for pulling the data or how it will be used. Moreover, the data holders never collected the data with the intent of the data being used for these purposes.

Section 1033 of the Dodd-Frank Act recognizes this challenge and provides limitations that make clear banks do not have these responsibilities in regard to aggregated data. The law requires banks to make available only data that are in the "control or possession" of the bank and explicitly exempts "any information that the covered person cannot retrieve in the ordinary course of its business." Section 1033 requires banks only to disclose the data that they already have. FCRA imposes further requirements on furnishers to curate data in a way that makes it specifically usable for credit reporting purposes.

Congress should urge the CFPB to coordinate with banking regulators in any rulemaking

Implementation of Section 1033 has wide-reaching implications for banks. Because of the sensitive nature of financial data, there are serious safety and soundness concerns that must be addressed. This is why Section 1033 requires the CFPB to "consult with the Federal banking agencies and the Federal Trade Commission," when prescribing any rules.

Conclusion

Today, technology is fundamentally changing the way financial services are being delivered. Consumer financial data are more available and more 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.



Statement by the Bank Policy Institute

Before the U.S. House Committee on Financial Services Task Force on Financial Technology
 "Preserving the Right of Consumers to Access Personal Financial Data"

September 21, 2021

Chair Waters, Ranking Member McHenry, Task Force Chair Lynch, Ranking Member Davidson and Members of the Fintech Task Force:

We support the ability of bank customers to securely connect their bank accounts to the third-party apps of their choice, which, in some cases, may involve the interposition of a data aggregator to collect the customer's information from the customer's financial institution and provide it to the app. It is critical, however, that consumers' personal and financial information remains secure when it is shared between financial institutions and third parties. Ensuring the security of customer data is, and will remain, a top priority for the banking industry. Consumer-permissioned financial data sharing should be guided by the following three principles:

- First, consumer financial information should be *safe and secure* regardless of who holds it;
- Second, *informed consumer consent* should be a precondition to any sharing of consumer financial information; and
- Third, the consumer should have *effective control* over the type and amount of information that is shared.

In light of these principles, we strongly support the migration of connections between financial institutions and data aggregators to secure Application Programming Interfaces, or APIs, that can support informed customer consent and control over their information and the secure transmission of this properly permissioned information.

We also support robust federal supervision and examination of entities like data aggregators and third-party data users that hold consumers' sensitive financial data.

Lastly, as it is the consumers' financial health and security that is at risk when their data is shared, the Consumer Financial Protection Bureau (CFPB) and other federal regulators should empower consumers to effectively control the sharing and use of their financial data. To do that, consumers need sufficient information and clear mechanisms of control in order to make informed decisions about: (i) the parties they are sharing their data with, (ii) the duration and frequency of permissioned access they are granting, (iii) the specific data elements they are sharing, (iv) the ability to revoke the access, (v) the ability to require third and fourth parties to delete their data, and (vi) the purposes for which third parties may use their data.

THE CURRENT STATE OF DATA AGGREGATION: OBSCURE AND INSECURE

Data aggregators play a key role in enabling fintech apps to access, aggregate, share and store information from banks and compile consumer financial account and transaction data. However, data aggregators work in the background, often unbeknownst to consumers, and the methods by which data aggregators collect and store consumer data puts consumers at risk.

After a consumer shares his or her credentials to facilitate access to a fintech app, aggregators are able to collect and store those credentials, and gain access to consumer data attributes through screen scraping activities. It is difficult to estimate the quantity of data held by data aggregators, of which there are approximately 120 in the United States. According to one report, data aggregator Acxiom provided up to 3,000 attributes on 700 million

people in 2017, and by 2018, it had collected 10,000 attributes on 2.5 billion consumers.¹ While these figures are difficult to verify, we can be certain that the largest data aggregators hold the sensitive financial information of millions of U.S. consumers.²

Unfortunately, many consumers lack an understanding of how their financial information is being collected, shared, and stored. A November 2019 survey conducted by The Clearing House (TCH), a banking association and payments company, found that more than 80% of financial app users are not aware that apps may use third parties to access consumers' personal and financial information, and 80% of financial app users are not fully aware that apps or third parties may store their bank account username and password.³

RISKS OF SCREEN SCRAPING AND CREDENTIAL-BASED ACCESS

The use of screen scraping and credential-based access is both outdated and unsafe. First, this method does not allow consumers to control the amount of data they share with third parties, and there is no way to ensure that the information "scraped" and maintained by the aggregator does not go beyond what is necessary for the financial app to deliver the services sought by the consumer. Additionally, there is the risk that the aggregator or third-party app may continue to collect and store the consumer's data and credentials even after the consumer ceases using the financial app.

Second, screen scraping, and the credential-based access on which it is based, creates opportunities for malicious actors to gain access to a consumer's accounts at a financial institution and commit fraud, or even take over the consumer's account. As former FinCEN Director Kenneth A. Blanco has previously warned: "In some cases, cybercriminals appear to be using fintech data aggregators and integrators to facilitate account takeovers and fraudulent wires. By using stolen data to create fraudulent accounts on fintech platforms, cybercriminals are able to exploit the platforms' integration with various financial services to initiate seemingly legitimate financial activity while creating a degree of separation from traditional fraud detection efforts."⁴

Third, screen scraping can divert the cybersecurity resources of regulated financial institutions away from preventing truly unauthorized access by criminals or other bad actors, because in many cases, it is difficult for a financial institution to distinguish "legitimate" data aggregator logins from illegitimate traffic. This problem is compounded by the fact that some data aggregators bypass security controls used by financial institutions to authenticate customer logins (such as by auto-populating the security questions posed when a new connection is sought to be established with a consumer's account). As the Basel Committee on Banking Supervision found in its 2019 "Report on open banking and application programming interfaces": "Screen scraping or reverse engineering can undermine a bank's ability to identify fraudulent transactions, as banks cannot always distinguish between the customer, data aggregator, and an unauthorised third party that is logging in and extracting sensitive data."⁵

MIGRATION TO APIS FOR CONSUMER FINANCIAL DATA SHARING

The use of APIs for consumer permissioned financial data sharing is widely considered to be more safe and secure than screen scraping, as APIs allow data to be shared without the use of consumer credentials and provide enhanced control over the type and extent of data shared. Several industry efforts have advanced the adoption of APIs in the United States. For example, the Financial Data Exchange developed a common API technical standard for data sharing through an industry consortium of banks, data aggregators, fintechs and consumer groups. Over

¹ <https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information>.

² Natalie S. Talpas, PNC Bank, Consumer Financial Protection Bureau Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act, Feb. 26, 2020, available at: https://files.consumerfinance.gov/f/documents/cfpb_talpas-statement_symposium-consumer-access-financial-records.pdf

³ The Clearing House, Consumer Survey: Financial Apps and Data Privacy, November 2019, available at: [2019-tch-consumersurveyreport.pdf](https://www.clearinghouse.org/2019-tch-consumersurveyreport.pdf) ([theclearinghouse.org](https://www.clearinghouse.org)).

⁴ Prepared Remarks of Fincen Director Kenneth A. Blanco, delivered at the Federal Identity (FedID) Forum and Exposition, "Identity Attack Surface and a Key to Countering Illicit Finance", (September 24, 2019), available at <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-federal-identity-fedid>

⁵ Basel Committee on Banking Supervision, "Report on open banking and application programming interfaces" (November 2019), available at: [Report on open banking and application programming interfaces \(APIs\) \(bis.org\)](https://www.bis.org/openbanking/20191101-report-on-open-banking-and-application-programming-interfaces-apis.htm).

22 million consumers are now using FDX's API for data sharing in North America.⁶ Additionally, banks and data aggregators have entered into data access agreements to facilitate the data sharing process through APIs and to specify how data is accessed and protected.

Despite the industry's progress, screen scraping remains a widely used method for accessing payments account data, enabling data harvesting of credentials to continue. Government action to outlaw screen scraping, either through an act of Congress or coordination between the CFPB and the federal banking agencies in implementing section 1033 of the Dodd-Frank Act, which provides the CFPB with authority to promulgate rules around consumer financial data sharing, would accelerate the migration of consumer data sharing to APIs. The technology exists today to migrate to APIs, but market participants may not have the incentive to transition to APIs if screen scraping is allowed to continue. The migration of thousands of banks, data aggregators and fintechs in the United States to APIs for sharing consumer data would be a significant undertaking, particularly for those banks that may not have actively participated in the market-driven movement towards APIs that has occurred to date. Indeed, this process could take several years to complete. For this reason, it is critical to establish a specific timeline *now* to end screen scraping so that all market participants begin to work towards a future ecosystem wherein all consumers are able to share their information on an informed basis in a safe and secure manner.

DATA AGGREGATORS SHOULD BE SUBJECT TO SYSTEMATIC CYBERSECURITY OVERSIGHT

Under the current framework, data aggregators access and store similar information to that of banks, but are not held to similar standards for safeguarding consumer data. The CFPB has the authority under the Dodd-Frank Act to define the universe of larger nonbank participants in the data aggregator market. The CFPB should initiate a rulemaking under this authority, which would then give the Bureau the authority to supervise and examine those entities for compliance with applicable data security standards and consumer financial laws, just as banks are regularly examined for compliance with the GLBA's information security standards and consumer financial protection laws. Further, the FFIEC should apply these GLBA standards to data aggregators and other authorized entities. The FFIEC examination guidance on information security also could serve as a useful model for the Bureau in developing the appropriate information security standards for large nonbank data aggregators and data users.⁷

CONSUMER TRANSPARENCY AND CONTROL

Simply put, consumers should have full awareness and control over how their data is shared and used. To that end, consumers should be made aware that a data aggregator or other third party is being interposed between the customer's bank and a third-party app and of the accounts and data fields that will be accessed by data aggregators and data users. Consumers cannot make informed choices without transparent and readily accessible disclosures. As the CFPB stated in its principles for consumer-authorized financial data sharing, firms seeking to obtain consumer authorization for sharing their financial data should provide clear disclosures regarding the "identity and security of [the] party, the data they access, their use of such data, and the frequency at which they access the data ... throughout the period that the data are accessed, used, or stored."⁸

Consumers must have the ability to consent to share their financial data, and the ability to confirm, modify and revoke access once granted. As a minimum safeguard, data aggregators and data users should be required to periodically require consumer re-authorization to access consumer data. Perpetual access permissions unnecessarily put consumers and their data at risk. Ideally, data aggregators and data users should be required to obtain the consumer's additional affirmative consent before they are allowed to use the consumer's data for a secondary use not reasonably expected by consumers, thereby empowering consumers to control all the potential uses by permissioned parties of their data.

Similarly, consumers should also have control over the duration of their consent to a third party's accessing their

⁶ See [Financial Data Exchange \(FDX\) Reports 22 million Consumer Accounts on FDX API](#).

⁷ FFIEC, Information Technology Examination Handbook, Information Security Booklet, available at <https://ithandbook.ffiec.gov/it-booklets/information-security.aspx>

⁸ Consumer Financial Protection Bureau, "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation" (Oct. 18, 2017), Principle 6, available at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

data. Currently, many consumers are not aware that deleting an app from their phone does not revoke the app's ability (or that of the app's data aggregator, if any) to continue to access the consumer's financial data. Indeed, Federal Reserve Board Governor Lael Brainard has observed, "[w]hen a consumer deletes a fintech app from his or her phone, it is not clear this would guarantee that a data aggregator would delete the consumer's bank login and password, nor discontinue accessing transaction information."⁹

In addition, data minimization is a fundamental security principle: limiting the dissemination of sensitive data reduces the consumer's risk of exposure. Unfortunately, the natural incentives of data aggregators and data users may not necessarily be aligned with this principle. Consumers therefore should be able to limit what data a third party can access and the purposes for which the data may be used.¹⁰

The right to data deletion also is an important and effective way consumers can protect themselves from future data breaches. And while the CFPB's second principle states that "[t]hird parties with authorized access ... [should] only maintain such data as long as necessary," many data aggregators and data users do not make it easy for consumers to exercise this right, to the extent they provide this right at all.¹¹ Federal Reserve Board Governor Lael Brainard recognized this problem, noting that "[i]f a consumer severs the data access, for instance by changing banks or bank account passwords, it is also not clear how he or she can instruct the data aggregator to delete the information that has already been collected. Given that data aggregators often don't have consumer interfaces, consumers may be left to find an email address for the data aggregator, send in a deletion request, and hope for the best."¹²

CONCLUSION

BPI supports consumers' ability to access and share their personal financial data. It is of paramount importance that this data is shared based on informed consumer consent and effective consumer control over the type and amount of information that is shared and that the data is maintained in a safe and secure manner regardless of where, why or with whom that data is maintained.

⁹ Lael Brainard, "Where Do Consumers Fit in the Fintech Stack?" (Nov. 16, 2017), available at

<https://www.federalreserve.gov/newsevents/speech/brainard20171116a.htm>.

¹⁰ Consumer Financial Protection Bureau, "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. Principle 2 states that participants should "only access the data necessary to provide the product(s) or service(s) selected by the consumer."

¹¹ *Id.*

¹² See note 8, *supra*.



September 21, 2021

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

The Honorable Warren Davidson
Ranking Member
Task Force on Financial Technology
House Financial Services Committee
4340 O'Neill House Office Building
Washington, D.C. 20024

Dear Chairman Lynch and Ranking Member Davidson:

On behalf of Envestnet Yodlee ("Yodlee"), thank you for holding today's hearing in the House Financial Services Committee's Task Force on Financial Technology ("the Task Force") entitled "Preserving the Right of Consumers to Access Personal Financial Data." As a global consumer-permissioned financial data aggregator that has been enabling consumers with access to their data across a vast spectrum of different types of financial accounts for the past two decades, and whose services to large financial institutions are subject to examination by the U.S. federal banking agencies, Yodlee welcomes the Task Force's focus on this critically important issue.

The ability of consumers and small businesses to access and permission access to their financial data is the lifeblood of technology-enabled financial products and services. These products and services provide essential personalized assistance to the consumer or small business as they manage their financial wellbeing in ways they've determined are best suited to their need and situation. Regardless of their use case, or whether they are provided by a financial institution or a financial technology ("Fintech") firm, all financial technology products and services rely on the capability of their customer to share access to the components of their financial data that are necessary to effectively and responsibly deliver the intended product or service.

Yodlee is the global market leading platform provider for consumer-permissioned financial data access. For the past twenty years, Yodlee has provided consumer-permissioned account aggregation capabilities with hosted solutions and commercial APIs on a business-to-business basis to customers around the world. We are proud to count 15 of the largest 20 U.S. financial institutions as our customers. Both traditional financial institutions and Fintech companies use Yodlee's platform to allow consumers to access and share their financial data across a myriad of legally permissible use cases. All of this is done to give consumers options for improving their own financial wellness as only those individuals themselves can truly appreciate. In this way, the Yodlee platform has been used to access over 470 million financial accounts and given consumers the choice to engage with financial management, advice, and lending solutions they themselves have selected as best suited to help them achieve their financial goals.



Yodlee is a strong advocate of a rulemaking under Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (“the Dodd-Frank Act”) by the Consumer Financial Protection Bureau (“CFPB” or “the Bureau”) and was encouraged by the inclusion of language in President Biden’s recent Executive Order on Promoting Competition in the American Economy encouraging the Bureau to act on its Section 1033 authority.¹ From our perspective as a critical enabler of consumer-permissioned data access across the financial services ecosystem, a CFPB rulemaking under Section 1033 presents the important opportunity to: provide consumers with a legal right to access and share access to their financial data that would facilitate greater competition and improved financial access and inclusion; ensure regulatory oversight of the Fintech marketplace; and, better protect consumers from misuse or mishandling of their data.

While the Bureau has had the statutory authority under the Dodd-Frank Act to promulgate a rule under Section 1033 for over a decade, we appreciate that the CFPB has taken a cautious approach to date in utilizing that authority. In so doing, the Bureau has allowed the market to develop without direct regulatory intervention and thus fostered the evolution of an authorized data access ecosystem that market participants have worked together to create. This approach has seen the relevant stakeholders come together to ensure consumer financial data sharing in a safe and secure manner that provides for a consumer protective ecosystem facilitated by newer, safer, and more efficient technologies to enable consumer financial wellness.

Despite industry collaboration in recent years towards a more consumer-centric financial data access ecosystem, the ability of consumers and small businesses to access and permission access to their financial data is not ubiquitous. A combination of areas, including regulatory ambiguity, legal requirements, and, in some cases, competitive concerns, has created a system in which some consumers have more utility over their own financial data than others, as well as more or less protection depending on the data access platform used to provide the access. A rule implementing Section 1033 of the Dodd-Frank Act is, in our view, an appropriate remedy to address this uneven playing field. Furthermore, the codification of applicable parameters for and supervision of certain market participants has the potential to solidify a new era of consumer financial wellbeing and to serve as the standard that burgeoning international markets around the world look to as they wrestle with similar questions. The cornerstone of any CFPB rulemaking under Section 1033 of the Dodd-Frank Act therefore must be a legally binding, absolute right for consumers to access and permission access to their banking and other financial transaction information safely and securely in real time.

The provision of this legal right for consumer data access represents the only pragmatic way to ensure that all consumers have the same financial opportunities and protections regardless of the financial institutions with which they choose to do business. Efforts within the financial services industry to achieve this outcome on its own, though they have progressed within the last 24 months, are simply moving too slowly to achieve this outcome. To wit: Yodlee has spent

¹ <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/>.



significant time and resources negotiating and executing bilateral data access agreements with many of the largest financial institutions in the United States but sees no easy means of executing similar agreements with the thousands of smaller financial institutions across the country. The disparate outcomes for consumers based on what data their financial institution makes available under these bilateral data access agreements – or whether their financial institution has struck any agreements at all – provides a compelling case for the Bureau to implement a customer data access right under its Section 1033 authority that provides the consumer access to any non-proprietary element of data held about them by a financial institution that they have created in the course of being a customer of that institution.

With this right provided, consumers and regulators should have greater assurances that financial data access is being facilitated safely and securely. To provide for consumer protection in this open finance environment, Yodlee would underscore a recommendation it has provided to the Bureau repeatedly over the last several years: data aggregation firms should be required to adhere to the data protection and privacy requirements of the Gramm-Leach-Bliley Act and to submit to supervisory oversight by the CFPB. Such a requirement should improve regulatory oversight of the consumer financial data ecosystem, and also should require that data aggregators exert governance over the customers on their platforms through the application of third-party partner risk management-like standards.

Supervision of data aggregation platforms is not only a critical component towards consumer protection, it also will meaningfully address an existing limitation of the marketplace to facilitate more fulsome consumer data access. Banks, credit unions and other providers of core transaction accounts in their role as data holders are subject to a litany of prudential regulation. Unfortunately, the lack of clarity with respect to the application of these concepts on the other covered persons in the marketplace has created a situation in which disparate obligations and rules applicable to only the existing subset of data holders is causing harm and increased cost both real and yet unrealized to the consumer.

As the covered data holders explicitly subject to existing laws have worked with other industry participants to harmonize the means and rules of access, they understandably have also sought to codify duties and obligations on the other market actors who are connecting to their systems to ultimately provide financial data at the request of the consumer. The absence of clarity with respect to what types of obligations and responsibilities sit with each data user downstream has caused absorption of risk and liabilities on these other market participants that runs the risk of stifling innovation and limiting competition. Unfortunately, guidance published by prudential regulators in this space to date has only served to exacerbate the likelihood of further restrictions to consumer data access by increasingly placing responsibility for oversight of the permissioned data access marketplace on data holders.²

While the prudence of applying these types of rigors on data aggregators is obvious, the only way for existing regulated data holders to satisfy their own regulatory obligations is manifesting

² See, for example, <https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html>.



itself in the current market through absorption of the requisite requirements on those seeking consumer data access. In the absence of regulatory obligations on data aggregators across the entire chain of market participants, data holders are requiring as a precondition of establishing connectivity with their institution that data aggregators agree contractually to absorb financial liability associated with any and all risks which could manifest through the release of consumer financial information across the downstream ecosystem.

Asking data aggregators to exercise diligence on each data user downstream absent clear examination guidance is untenable and ineffective given the large and growing number of Fintech market participants. Faced with these unevenly applied contractual obligations, each data aggregator has necessarily implemented its own process of governance and oversight of the data users on its platform. With our decades of experience being subject to our own regulatory obligations in this market, it has given us an appreciation for how the existing frameworks can actually be leveraged to meet and ultimately uplift all market participants without undue burden on any one particular subgroup.

The issue being examined by the Task Force at today's hearing lies at the heart of the ability of the financial services ecosystem to provide consumers and small businesses with technology-enabled tools that improve financial access, inclusion, and outcomes. While the industry has made strides in recent years towards increased financial data access for consumers, Yodlee strongly believes that the CFPB should utilize its Dodd-Frank Section 1033 authority to: promulgate a legally binding data access right for consumers; create a supervisory regime for data aggregators; and, set forth guidance for aggregators' downstream Fintech customers with regard to minimum compliance standards. This approach would provide consumers across the country with universal access to their own financial data in a safe, secure, and regulated ecosystem, and would thus herald in an era of open finance in the United States.

Once again, thank you for holding today's hearing on this critically important topic.

Sincerely,

Chad Wiechers

Chad A. Wiechers
Senior Vice President, Data Access & Management
Investnet Yodlee



Financial Data and
Technology Association

<http://www.fdata.global/north-america>

VIA ELECTRONIC SUBMISSION

September 21, 2021

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

The Honorable Warren Davidson
Ranking Member
Task Force on Financial Technology
House Financial Services Committee
4340 O'Neill House Office Building
Washington, D.C. 20024

Dear Chairman Lynch and Ranking Member Davidson:

The Financial Data and Technology Association of North America ("FDATA North America") appreciates this opportunity to submit a letter for the record for the House Financial Services Committee's Task Force on Financial Technology's hearing "Preserving the Right of Consumers to Access Personal Financial Data." As the leading trade association representing financial data aggregation firms and financial technology platforms that provide enhanced consumer financial access and inclusion, FDATA North America and its member companies strongly believe and advocate for a financial ecosystem in which the end user has complete utility of their financial data.

About FDATA North America

FDATA North America was founded in early 2018 by several firms whose technology-based products and services allow consumers and SMBs to improve their financial wellbeing. We count innovative leaders such as the Alliance for Innovative Regulation, API Metrics, Basis Theory, Betterment, BillGo, Codat, Direct ID, Equitable Bank, Envestnet Yodlee, Experian, Fiserv, Flinks, Interac, Inverite, Intuit, Kabbage, Mogo, Morningstar, M Science, MX, Petal, Plaid, Qeustrade, Rocket Mortgage, Salt Edge, Trustly, ValidiFI, VoPay, Wealthica, Xero, and others among 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 and policy expertise to policymakers and to regulatory bodies internationally that are contemplating, designing, and implementing open finance frameworks. With chapters in North America, Europe, Australia, South America, and India, FDATA Global has established itself as an expert in the design, implementation, and governance of open finance standards and frameworks globally since its inception in 2013.



<http://www.fdata.global/north-america>

FDATA North America’s members include firms with a variety of different business models. Many provide technology services to large financial institutions or partner with financial institutions to enable innovation and expand financial access and inclusion. Others offer their own customer-facing financial products or services that may, for example, expand access to low-interest credit for thin or no-file borrowers, provide a gateway to automated savings or investments, onboard SMBs to accept and make digital payments, or support the SMB community by enabling technology-powered advisory and accounting services. Collectively, our members enable tens of millions of American consumers and SMB customers to access vital financial services and products, either on their own or through partnerships with financial institutions. Regardless of their business model, each FDATA North America member’s product or service shares one fundamental and foundational requisite: it depends on the ability of a customer to actively permission access to some component of their own financial data that is held by a financial institution.

The Need for CFPB Rulemaking Under Section 1033 of the Dodd-Frank Act

FDATA North America has, since its inception, encouraged the Consumer Financial Protection Bureau (“CFPB” or “the Bureau”) to utilize the authority vested in it under Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (“the Dodd-Frank Act”) to promulgate, by rule, a consumer financial data right that will spur greater financial services innovation and competition and improve consumer financial access and inclusion. We have been encouraged by two important developments to this end in recent months: the issuance of an advance notice of proposed rulemaking (“ANPR”) by the Bureau pertaining to consumer access to financial records late last year and, more recently, inclusion in President Biden’s July 2021 Executive Order on Promoting Competition in the American Economy language that encourages the CFPB to consider “commencing or continuing a rulemaking under section 1033 of the Dodd-Frank Act to facilitate the portability of consumer financial transaction data so consumers can more easily switch financial institutions and use new, innovative financial products.”

The drumbeat towards the promulgation by the CFPB of a rulemaking under Section 1033 of the Dodd-Frank Act comes at a critical moment. Countries around the world are quickly embracing the notion that the customer should be in control of their own financial data. By contrast, the unlevel playing field that currently exists for consumers and small- and medium-sized businesses (“SMBs”) in the United States in this regard represents both a failure to American consumers and SMBs as well as a global competitive disadvantage. This unlevel playing field has, to date, been dictated by opaque bilateral data access agreements between their financial institution and aggregation firms that enumerate what choices they have to utilize their own financial data and the protections they are afforded when they do so.



<http://www.fdata.global/north-america>

This problematic reality endures because, unlike a growing list of other large economies across the globe, there exists no distinct assertion of a customer's legal right to access themselves, or permission access to, their financial data in the United States. Although Section 1033 of the Dodd-Frank Act establishes a direct financial data access right for consumers, unless that data right includes authorized data access to third parties chosen by the consumer, it will provide inadequate access to critical financial products and services. The status quo, under which financial institutions continuously exercise control over their customers' data, provides little benefit to the consumer or SMB. Financial institutions have historically used this control to determine whether and how their customers may utilize third-party financial services providers, including outright blocking the ability of their customers to do so. While, in some cases, financial institution throttling or blocking of third-party tools may be positioned as being based on security or regulatory compliance postures, competitive concerns unquestionably have fueled some of this behavior as well. In these instances, the end user typically is unaware as to why the product or service they are trying to use – or even have depended on for their financial wellbeing in the past – is not functioning or supported. This artificially stifles both consumer choice and marketplace competition.

Additionally, FDATA North America sees competition in data-driven financial services stifled by financial institutions that override customer direction to authorize sharing of their financial data. These restrictions include broad, as well as specific, attempts to directly limit third parties' access to data despite customer authorization; degradation of data sharing that effectively thwarts customer-directed access to financial data; and self-imposed mandatory reauthentication requirements and targeted blocking of sharing specific data fields in ways that effectively disable competing services. A recent FDATA North America study determined that more than 650 million existing consumer and small and mid-size accounts held by tens of millions of customers in the United States could be rendered useless by industry-led initiatives to move to APIs at just the largest 25 financial institutions.¹ These institutions do not supply sufficient data to fuel existing use cases upon which customers depend to manage their financial wellbeing. In each of these cases, competition in data-driven financial services would be substantially inhibited, to the direct and severe detriment of consumers. Recent investments by the largest financial institutions in the U.S. in a commercial entity that seeks to grant greater control to data holders regarding whether and how they will abide by their customers' instructions to grant access to their financial data have further eroded faith in the third-party provider marketplace that industry alone can deliver the outcome envisioned by Section 1033 of the Dodd-Frank Act.

Aside from competitive concerns, the logistics of providing customer-permissioned data access have become a significant blocker to a more vibrant marketplace. A growing number of large

¹ Please refer to Appendix A.



<http://www.fdata.global/north-america>

U.S. financial institutions are requiring third parties to negotiate and execute bilateral data access agreements if they desire to establish customer-permissioned data connectivity. While these bilateral agreements are intended to provide critical governance in banks' transitions from existing data-gathering technologies to the use of APIs, and have been encouraged based on recent supervisory guidance by the Office of the Comptroller of the Currency ("OCC")², market participants generally recognize that individually negotiated bilateral agreements are an inefficient means over the long term of dealing with customer-permissioned data access. Such agreements lack uniformity, transparency, and insight, which can be challenging and expensive for third-party partners. These agreements result in differences between direct access and authorized access to desired tools by consumers based on the institution with which they have banking relationships and the aggregator that provides the services to the desired tool.

Several FDATA North America member organizations that have executed data access agreements with large financial institutions report that the negotiations can take as long as three years to execute and often require extensive legal costs. Smaller financial institutions will not bear such costs and are thus discouraged from adopting new technology and user services. Additionally, the technology lift and technical resources required to develop independent APIs is a disincentive to smaller financial institutions that desire to allow their customers to permission access to products and services that they do not offer. An ongoing dependence on bilateral data access agreements therefore presents a significant challenge to smaller financial institutions that will struggle to keep pace with larger banks nationwide regarding API integration due to the substantial expense of negotiating bespoke agreements with any third party wishing to connect to that API.

Any fair assessment of the ecosystem must also conclude that, in the absence of a legally binding mandate to make customer data available with that customer's consent, commercial interests can factor into decisions that financial institutions make regarding what data to include in their APIs or how onerous the terms of third-party bilateral agreements will be. One of the principal rationales for government-led open finance regimes is the fact that holders of a customer's financial data, who themselves have a commercial interest in retaining that data to offer their customer additional financial products or services, have a competitive disincentive to make that data available because they use it offer their customer additional financial products or services.

Principles for Ensuring Consumer and SMB Financial Data Access

The CFPB has, through its Section 1033 authority, the opportunity to significantly level the playing field for consumers and SMBs, expand financial access and inclusion, improve

² "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29." March 5, 2020. <https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html>.



<http://www.fdata.global/north-america>

competition in the financial services marketplace and, on a global level, ensure that the United States' financial services system remains competitive internationally. To accomplish these critically important objectives, FDATA North America has recommended to the Bureau that it utilize its Section 1033 authority to issue a rule that adheres to six key principles:

1. **The CFPB should create a legal customer financial data right.** FDATA North America strongly believes that any non-proprietary data element that is available to a consumer or SMB through their online banking portal or is included on a paper statement, and that is not the intellectual property of the data holder, should be considered in scope as the Bureau contemplates promulgating a customer financial data right under Section 1033 of the Dodd-Frank Act.
2. **The Bureau should define and clearly enumerate the limited circumstances in which custodians of financial data may override customer consent.** The Bureau should prescribe a well-defined set of circumstances under which financial institutions may withhold or restrict access to a customer's data access right to avoid a suppression of customer choice, voice, and consent. These circumstances should be limited to instances in which a data access request poses an imminent security risk or a situation in which the financial institution, the aggregator, and the customer each reasonably understands why the holder of the data determined that it was not in the consumer's or SMB's best interest to share the data due to evidence that the entity to which the customer permissioned access to their data posed a clear risk to the customer's financial wellbeing. Importantly, defining the circumstances under which a data holder may restrict data access would prohibit financial institutions from limiting their customers' ability to access their financial data for any other reason.
3. **The CFPB should directly supervise financial data aggregation firms.** The best way to address financial institutions' concerns regarding third-party supervision issues associated with financial data access, and to remove the need for onerous bilateral data access agreements, is for the Bureau to create a federal supervisory regime for data aggregation platforms. Such a supervisory regime should establish a principles-based baseline for data, cyber, and information security practices as well as governance over aggregation firms. Importantly, direct supervision of data aggregation platforms would also enable the CFPB to exert third-party partner supervisory standards for aggregators' fintech clients.
4. **The Bureau should coordinate with the prudential regulators on Regulation E modernization.** Regulation E was first promulgated to address financial institutions' liability to their customers when ATMs became commonplace in the 1970s. Innovation in



<http://www.fdata.global/north-america>

the financial services ecosystem has outpaced a liability framework that never could have envisioned an environment in which customers could permission access to their financial data electronically to third parties in real time. To ensure liability is appropriately allocated throughout the financial ecosystem, FDATA North America advocates for a modernization of Regulation E that stipulates that the entity responsible for customer loss of funds related to a data breach or fraud be responsible for making that customer whole based on custody and responsibility.

5. **The CFPB must recognize the need to permit current and legacy technology.** While FDATA North America is technology neutral and supports the transition to application programming interface (“API”) access of customer-permissioned financial data, it is important to acknowledge the reality that the financial ecosystem is not yet ready to completely prohibit existing technological methods of accessing customer data without massive detriments to consumer and SMB financial health. In the absence of a fully developed, robust API environment, direct access, sometimes also referred to as “screen scraping” of the consumer interface, is a necessary tool to enable consumer and SMB data access, particularly for customers of all but the largest U.S. financial institutions. In Europe, the transition to its modernized second payment services directive (“PSD2”), which supported full consumer utility over their financial data, recognized the benefits of API access but embraced screen scraping as a fallback option in the event that APIs were not readily accessible for covered data fields. This approach has the benefit of providing an incentive for banks to build robust APIs more quickly; poorly designed and implemented APIs that are deployed into the market will simply not be fit for purpose.
6. **A strong federal data privacy regime would benefit consumers and SMBs.** While the Bureau is not granted under Section 1033 of the Dodd-Frank Act the authority to promulgate a national data privacy regime, FDATA North America and its members offer that such a framework would be additive to consumer and SMB protection and would better align the United States with other jurisdictions, including Europe, that have implemented national or supranational data privacy requirements.

The combination of these six principles would provide consumers and SMBs with safe, secure access to their financial data and, by extension, to critically important financial applications and tools that can meaningfully improve their financial wellbeing.



<http://www.fdata.global/north-america>

Conclusion

FDATA North America appreciates the attention to this critically important issue by the Task Force on Financial Technology. Every financial technology tool, regardless of its specific use case, depends on the ability of its customer, whether they are a consumer or SMB, to grant access to components of their financial data in order to provide the benefit of their product or service. Accordingly, limitations, restrictions, or outright blocking of financial data access to consumers and SMBs threatens the ability of financial technology tools to support their customers' financial wellbeing and stifles innovation in the financial services marketplace.

As the CFPB works to promulgate a proposed rule under Section 1033 of the Dodd-Frank Act, we hope that the Task Force on Financial Technology will continue to examine this vitally important space and encourage the Bureau to use its statutory authority to create a customer-centric, safe and secure open finance system in the United States.

Thank you once again for holding today's hearing.

Sincerely,

A handwritten signature in black ink, appearing to read "S Boms", with a long horizontal line extending to the right.

Steven Boms
Executive Director
FDATA North America

Enclosure



<http://www.fdata.global/north-america>

Appendix A: Missing API Data Fields and End User Impact^{3 4}

<i>Financial Institution Size, By Total Assets</i>	<i>Impacted Use Cases</i>	<i>Total Number of End User Accounts Impacted</i>
Top 10	Consumer Personal Financial Management, Account Verification, Lending, Small Business; Money Management, Money Movement, Wealth Management, Retirement Savings, Tax, Bookkeeping, Loan Underwriting, Fraud	557,395,494
11-25	Consumer Personal Financial Management, Lending, Small Business, Money Movement, Wealth Management, Retirement Savings, Tax, Bookkeeping, Loan Underwriting, Fraud	103,572,965

³ As of December 1, 2020.

⁴ Because some of the largest 25 U.S. financial institutions have not yet implemented an API, data is extrapolated to reflect the total impact to end users if those APIs, once established, mirror those that have already been deployed by other large financial institutions.



**Statement of Penny Lee
Chief Executive Officer
Financial Technology Association**

**before the
HOUSE FINANCIAL SERVICES COMMITTEE
TASK FORCE ON FINANCIAL TECHNOLOGY**

September 21, 2021

The Financial Technology Association (FTA) applauds the House Task Force on Financial Technology for holding an important hearing on “Preserving the Right of Consumers to Access Personal Financial Data” and appreciates the opportunity to submit a statement. In early 2021, the Consumer Financial Protection Bureau (CFPB) announced its intention to commence a rulemaking on Section 1033 of the Dodd Frank Act, and a recent Presidential Executive Order directs the CFPB to pursue this rulemaking with the purpose of unlocking further financial innovation and choice for consumers. FTA strongly supports the consumer-centric implementation of open banking regulation in the United States to empower consumer choice, preserve data security, and ensure consumer privacy.

Open banking allows consumers to safely and securely access and share their financial data across financial services providers to obtain greater financial choice, personalization, and outcomes. Open banking is rooted in the acknowledgment that consumers own their financial data and can share it with another financial service provider to access various financial benefits.

Once a consumer selects a financial application or provider, they can share their data through two primary methods: the use of secure application programming interfaces (APIs) or by screen scraping, whereby consumers can share their information (user-name and password) with a trusted third-party to access the necessary data on their behalf. While the ecosystem is moving towards API-based access, with some of the largest financial institutions developing APIs in recent years, it is important to note that screen scraping is the primary method by which the large majority of banks are currently able to share consumer data.

Open banking allows consumers more convenient and efficient ways to view and manage their money and shop for more customized and lower-cost financial services products and providers. It facilitates competition by allowing new entrants in the marketplace and ensures information is no longer trapped with incumbent providers. Open banking allows access to essential tools for



unbanked and underbanked consumers, including increased access to credit through identity verification, data sources, such as rental, utility, tax payment history, and no-fee salary advances.

Recent research highlights the rapid growth of open banking in Europe, where consumers use APIs to share their payment data and where access to new services is expected to double from 2018 through 2021.¹ Early data out of the UK demonstrates that open banking is driving growth in the number of regulated third-party providers.² Open banking and the seamless and secure flow of permissioned data allows fintech companies to offer consumers tailored and improved services; a recent survey found that 73% of Americans say fintech gives them more control over their finances and 68% say it helps them reduce financial anxiety.³ Another recent survey of consumers found that 77% would value having their financial institution offering them personalized financial advice based on open banking data and 94% would want their financial institution to use financial data to advise them about a better deal on a product.⁴

FTA believes in well-regulated open banking platforms that allow free-flowing information, subject to privacy and security guardrails, to give consumers complete ownership of their financial data. However, it is essential that regulation recognizes and supports the value of financial information in promoting improved, tailored, and more accessible financial products and services. Arbitrary limitations on data usage will chill beneficial innovation that drives clear consumer benefit, including the elimination of overdraft fees, greater access to credit, and lower costs. To this end, FTA encourages regulators and policymakers to:

- Establish a broad data right that is consistent across direct and authorized access;
- Create a level playing field for all Americans and ensure that Section 1033 rulemaking does not generate inequity for consumers, where consumers' access differs depending on where they bank;
- Allow for the free flow of data from other institutions that touch a consumer's financial life, including payroll companies, telecom, and utility providers, and the government, which can provide, for example, Social Security data;

¹ Juniper Research, *Open Banking Users to Double by 2021, as Consumers Seek Deeper Financial Insights* (May 19, 2020), available at <https://www.juniperresearch.com/press/open-banking-users-to-double-by-2021-as-consumers>.

² McKinsey, *Financial services unchained: The ongoing rise of open financial data* (July 11, 2021), available at <https://www.mckinsey.com/industries/financial-services/our-insights/financial-services-unchained-the-ongoing-rise-of-open-financial-data>.

³ Plaid/Harris Poll, *The Fintech Effect: Consumer Impact and the Future of Finance* (2020), available at <https://plaid.com/documents/the-fintech-effect-2020-consumer-report.pdf>.

⁴ MX, *The Ultimate Guide to Open Banking*, available at <https://www.mx.com/ultimate-guides/open-banking/>.



- Establish strong guidelines for consumer transparency and control, including that consumers be aware of all parties involved in data sharing and have ownership over which data they are sharing, with whom, and for what duration; and
- Support standards-development in service of consumer rights by establishing baseline principles and expectations that those standards must meet.

FTA appreciates the opportunity to provide comment in this important discussion and looks forward to serving as a resource to this Committee.

Sincerely,

A handwritten signature in black ink that reads "Penny Lee". The signature is written in a cursive, flowing style.

Penny Lee
CEO
Financial Technology Association



Statement for the Record
House Financial Services Committee
Task Force on Financial Technology

"Preserving the Right of Consumers to Access Personal Financial Data"

September 21, 2021

10:00 a.m.

Introduction

Pinwheel was founded in 2018 with the mission to create a fairer financial system by unlocking consumer access to their payroll information. In 2019, Pinwheel built the first application programming interface (API) into payroll platforms, and by 2020, Pinwheel was integrated with every major payroll provider and gig economy platform, covering roughly 70% of paid Americans. Over half of the direct deposit switches in the neobank marketplace will be completed through Pinwheel's API by the end of 2021, making it one of the most powerful tools available to consumers who require the safe and efficient flow of payroll data to effectuate a financial transaction.

We appreciate the Task Force's efforts in this area and agree that the right of a consumer to access their personal data *and* permission the use of that data should be preserved *and* expanded. As the Consumer Financial Protection Bureau (CFPB) acknowledged in the announcement of their advanced notice of proposed rulemaking:

"When consumers use financial products and services, the providers of those products and services generally accumulate data about those consumers and their use of those products and services. Consumer access to these data allow consumers to manage their financial accounts and can enhance consumers' control of their financial matters. Consumers may realize these benefits by authorizing third parties to access these data on their behalf and allowing those third parties to deliver new or improved financial products and services. Use cases for consumer-authorized data include personal financial management, making and receiving payments, assisting consumers with improving savings outcomes, underwriting credit, and many other services."¹

For this statement, we focus on the following policy areas:

- Payroll data must be included in the definition of financial data and ultimately, Payroll providers must be included in the definition of "data holder."
- There are both benefits to the consumer of including payroll data and consequences of NOT including payroll data within the definition of "consumer financial information."
- When crafting the regulation, consumer permissioned access and security of that data are of utmost importance.

CFPB 1033 ANPR

The CFPB is in the middle of a consequential rulemaking process that will set the terms for how consumers can take control of their financial data in the future. Section 1033 of the Dodd-Frank Act directed the CFPB to draft rules that require a data holder to grant consumers access to their data that is held by the data holder. The law gives the CFPB considerable latitude to determine the details of these rules.

¹<https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-releases-advance-notice-proposed-rulemaking-consumer-access-financial-records/>.

This is a policy issue that the CFPB has been exploring for some time. In 2017, the CFPB issued a set of principles on data access². In 2020, the CFPB put out a call for comments³ on Section 1033 in an advanced notice of proposed rulemaking (ANPR) and received almost 100 comments from industry groups and other stakeholders. Within its ANPR, the CFPB defines “financial data” as “information in the control or possession of [a] covered person concerning a consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account, including costs, charges and usage data.”

Payroll data and ultimately payroll providers should be included within the CFPB’s 1033 rulemaking

Pinwheel holds the position that a consumer’s financial data belongs to the consumer regardless of the institution that holds it. The data on income and employment stored in payroll systems is financial information; given that classification and the significant benefits unlocking it can offer consumers, we believe the CFPB should make explicit the inclusion of payroll data in Section 1033 and ultimately that payroll providers must be included in the definition of a “data holder.” Doing so will accelerate the innovation enabled by payroll connectivity, ultimately expanding access to financial products and services for all Americans.

To accomplish this goal, CFPB should include as a subset of “financial data,” a definition of “consumers’ payroll information.” In line with other industry stakeholders, we would recommend the following:

“Consumer Payroll Information means (1) any data that is (A) in connection with a consumer’s status or terms or condition of employment, such as whether the consumer is employed, is paid by an hourly rate (including such rate of pay), is a salaried employee or officer, or is a full-time or part-time employee; (B) related to accrued wages, deductions for benefits, frequency or timing of payment of wages or salary, tax information, or other data related to the processing of such payments; or (C) contained in, or related to, the employer’s file of data about a consumer, such as the consumer’s contact information. Without limiting the scope of paragraph (1)(C), any data about a consumer that is collected by a Payroll-Services Provider, or collected by an employer which forwards the data to (or makes the data accessible to) the Payroll-Services Provider, constitutes Consumer Payroll Information.”⁴

²https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

³<https://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-releases-advance-notice-proposed-rulemaking-consumer-access-financial-records/>.

⁴<https://www.regulations.gov/comment/CFPB-2020-0034-0083>.

Benefit of including Payroll data in “consumer financial information”

While access to consumer banking data has been a key driver in innovation over the last decade, payroll aggregation is the next step in the evolution of financial account connectivity, as it means retrieving income & employment data directly from the source and giving consumers the ability to edit their payroll account settings. More than 93% of US workers get paid via direct deposit⁵, meaning that payroll systems sit at the top of the financial stack and are essential to painting a holistic view of a consumer’s financial life. Unlocking access to this information helps drive innovation that could better serve the millions of Americans left behind by our financial system due to antiquated processes and technologies. It provides meaningful benefits to users, including the abilities to:

- Quickly and easily switch their direct deposit between financial institutions, taking control of their paycheck at the source and choosing the institution that offers them the best products and services.
- Share the wealth of income and employment data stored within a payroll system with financial institutions, unlocking lower-cost services. *More than half of the population has a poor credit score or no credit score at all. The information in payroll platforms, like gross and net pay, length of employment, shifts, and title can be used by lenders to build a more complete profile of the borrower to expand their pool of serviceable applicants previously limited by underwriting models that only factor in FICO scores.*
- Set up repayments directly from their paycheck, reducing risk for the lender and potentially unlocking even lower-cost loans
- Use payroll data to verify employment for job applications, background checks and other use cases.

Consequences of NOT including Payroll data among Consumer Financial information

Payroll data informs the picture of a consumer’s income. At times, this data may be the only data available in one’s financial life. Nearly 1 in 10 adults in the United States are credit invisible. Without payroll data in hand, one with limited financial data or perhaps no financial history at all would only encounter additional challenges when trying to obtain financial services.

Additionally, as one of the commenters to the 1033 ANPR stated,

“Among other potential pitfalls, a consumer will face obstacles choosing how the consumer’s funds from an employer are credited to the consumer’s preferred bank account, and will pay higher costs for credit or deposit products—which adversely affects the consumer’s liquidity or savings—because banks and other financial institutions will not be able to use and analyze payroll data to gain insights the consumer’s earnings or work history.”⁶

⁵ <https://www.nationalpayrollweek.com/direct-deposit/>.

⁶ <https://www.regulations.gov/comment/CFPB-2020-0034-0083>.

Payroll providers should be included as “data holders” in CFPB regulations

A payroll services provider is responsible for processing one’s payroll and facilitating the transfer of that payroll from one’s employer to one’s designated bank account. The data that a payroll services provider holds include income and employment data. Payroll service providers can also be providers contracted through an employer. As the CFPB has the authority to regulate those “engaged in offering or providing consumer financial product or service”,⁷ the underlying duties of a payroll provider qualify.

That being said, because there has been some uncertainty as to whether or how payroll services providers fit under the CFPB’s authority, we’d recommend including a payroll service provider as a “data holder” or agent of the data, as defined in the CFPB’s 1033 ANPR.

We support the recommendation by a commenter to the 1033 ANPR:

“The rule should expressly cover, as one of many types of *Covered Persons* (or “*Data Holders*”), a *Payroll-Services Provider*, which should be defined along the lines of:

“(1) *Payroll-Services Provider* means any person that offers or provides to a consumer (primarily for personal, family, or household purposes), directly or indirectly including through any employer, any: (A) payment to the consumer (as employee, contractor, or any other capacity for the consumer’s performance of work or services); or (B) any data processing function, product, or service in connection with the collection of, classification or organization of, or provision or delivery to any person of Consumer Payroll Information.

“(2) *Exception. Payroll-Services Provider* shall not include a person that both: (A) directly employs the consumer in any capacity, including if the consumer is a salaried employee or officer; and (B) directly collects and maintains all such Consumer Payroll Information in the person’s information systems which are not controlled or maintained by any service provider to such person.”

The key for finding that a *Payroll-Services Provider* is subject to the requirements of the rule under § 1033 is to recognize that the person is providing to a consumer (primarily for personal, family, or household purposes) any payment to the consumer (e.g., wages) or data processing functions relating to *Consumer Payroll Information*, as described in the definition proposed above. The Bureau has ample authority under the CFP Act to determine that, by offering or holding out to a consumer these types of payroll products or services, a person is a *Payroll-Services Provider*, regardless of whether the person also has a contract in place to act as a vendor for the employer. Accordingly, the definition for a

⁷ 12 U.S.C. § 5481(6)(A).

Payroll-Services Provider must contain terms that are sufficient to defeat the false argument that a person's payroll activities may not be subject to the Bureau's rule under § 1033 because that person only serves the business interests of the employer; in this way, the definition proposed above states that a person qualifies as a *Payroll-Services Provider* if the person "offers or provides to a consumer [any of the covered products or services] . . . directly or indirectly including through any employer." The Bureau must not be deterred in regulating a *Payroll-Services Provider* under § 1033 by the circumstance in which the *Payroll-Services Provider* delivers its products and services, which center on the processing of *Consumer Payroll Information*, to both the employer and to the consumer."⁸

Including payroll service providers as "data holders" would enable employees to access and share this data on an ongoing basis (meeting the existing access requirements outlined in the proposed ANPR).

Data Security

We support the consumer's right to access their data in whatever manner they choose and with whatever application they desire. The key to this premise is the fact that it is based on whatever the consumer chooses. Consumers must have a clear understanding how their data is used and shared and affirmatively opt in to that data sharing. This is of utmost importance and the key tenant to permitting this data access for the industry.

Security of one's systems - and ultimately, the security of the data itself - is critical to the success of this regulation.

When a consumer authorizes data sharing through the Pinwheel API, we are working behind the scenes to protect personal and financial information. Our security policies and practices are designed to meet or exceed the industry standards that banks and leading technology companies use. They include:

- End-to-end data encryption: The combination of the Advanced Encryption Standard (AES-256) and Transport Layer Security (TLS) help keep personal information safe end-to-end.
- Strong authentication: Pinwheel protects user data on our systems and requires multi-factor authentication for added security.
- Cloud security: Pinwheel uses secure cloud infrastructure technologies to enable users to connect quickly and safely.
- Robust monitoring: Pinwheels API and all related components are continuously monitored by our information security team.

⁸ <https://www.regulations.gov/comment/CFPB-2020-0034-0083>.

- Regular third-party security audits: Industry-leading security firms regularly audit Pinwheel's API and security controls. All data belongs to the user. That means:
 - We don't sell user data to any outside companies.
 - We don't share user data with anyone without user permission.
 - The user is in control of whom they share their data with and for how long.

We are grateful to be at the forefront of innovation in a space that is long overdue for widespread transformation, and to work with regulators in promoting consumer protection and financial inclusion. We would be happy to answer any questions you may have on this statement or as you continue to examine this policy issue.

Statement of Katie Neal
Outreach and Advocacy Lead
Plaid, Inc.

before the
HOUSE FINANCIAL SERVICES COMMITTEE
TASK FORCE ON FINANCIAL TECHNOLOGY

September 21, 2021

Plaid appreciates the opportunity to submit a statement for the record concerning the hearing on “Preserving the Right of Consumers to Access Personal Financial Data” before the House Financial Services Committee, Task Force on Financial Technology. Plaid, Inc. (“Plaid”) is a financial technology network that enables consumers to access and share their financial data in order to power technological applications they use to improve their financial lives. Plaid has built data sharing integrations with over 11,000 financial institutions and 5,500 fintech companies, helping millions of consumers and small businesses access and share their data and reap the benefits of new and innovative digital financial tools. We offer services to both financial technology (“fintech”) companies and traditional financial institutions, and also provide consumer-facing applications to help consumers manage access to their financial data.

Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) was enacted to allow consumers to benefit from access to their own financial data by making it portable and giving the consumer control over sharing it with the different financial services providers of their choice. Thanks to the ability to share their data, consumers have been able to access an entirely new marketplace of personalized goods and services and experience benefits from low-cost remittances to overdraft protection to automated savings tools.

We are heartened to see Congressional agreement on the need for a 1033 rule and would welcome supervision of data aggregators as a key tenant of this rule. In order to ensure a robust 1033 rule that protects consumers, encourages competition, and allows for continued innovation in financial services, we recommend Congress monitor the rulemaking for consistency with three key policy goals.

1. Consumer Privacy and Transparency must be reinforced throughout the ecosystem.

Consumers should be aware of all parties involved in sharing their permissioned data and share consent with those parties. When consumers grant permission to access their data to a fintech application through digital means, it should be clear when there is a financial aggregator in the middle who is responsible for accessing this data. This is why we developed Plaid Link,¹ a product that lets consumers know that Plaid is acting on their behalf to retrieve their financial data and share it with the app of their choice.

In addition to APIs, current industry practices for data collection include screen scraping. In order to protect consumer privacy, Plaid believes screen scraping should not occur in the background

¹ <https://plaid.com/blog/setting-the-standard-for-safe-and-secure-data-access>

without consumer consent or collect extraneous data unrelated to powering a consumer's chosen application. As many Task Force Members have noted, disclosure is necessary but not always sufficient to ensure consumers are protected. Consumers should also have the right to only share the data used to power the service they want, to know what data is shared with which applications, to revoke access to the sharing of this data, and to have Plaid delete or revoke access to their data for any reason. Plaid offers these features on our Portal, which is still in beta, and we believe such tools should be industry standard.² Companies can also re-consent consumers on an annual basis to ensure they still wish to share their data and engage in proactive privacy measures.

2. All consumers should have full access to their own financial data, no matter where they bank.

Consumers have the right to choose to share their financial data with the safe and secure services they desire, and that right should not be limited by their bank's technological ability. As acknowledged in the hearing, the industry is aligned on the need to shift from credential-based screen scraping to Application Programming Interfaces (APIs), but policymakers must ensure that consumers do not lose access to financial services during this transition.

We have seen faster movement towards API from larger financial institutions, which the industry acknowledges that this is a costly and resource-intensive process. Smaller institutions like community banks and credit unions typically have substantially lower technology budgets than larger institutions³ and may fall behind if their customers want to use third party applications for which they can't provide connectivity.⁴ Last year, we launched Plaid Exchange,⁵ a low-lift API, to help speed along this transition for smaller institutions and allow for a secure, reliable method for their customers to connect accounts to apps and services, as well as provide the tools needed to manage and monitor these connections. Since launch, we have enabled core providers Jack Henry Banno⁶ and Q2⁷ to seamlessly allow banks on their platforms to integrate with our API.

While the financial industry actively works towards adoption of APIs through industry-lead bodies like the Financial Data Exchange (FDX), Congress and the Bureau should prioritize ensuring that consumers can maintain access to their financial data in the interim. Creative and flexible solutions are already live to act as stepping stones toward full API adoption. For example, Plaid has partnered with financial institutions to develop tokenized screen scraping methods, a technology that allows a consumer to access their account information without sharing their credentials with another party, permitting ongoing access while financial institutions build APIs.

² <https://my.plaid.com>

³ See, e.g., PYMNTS, JPMorgan, BoA Lead US Bank Tech Spending (Mar. 29, 2019), <https://www.pymnts.com/news/b2b-payments/2019/jpmorgan-bank-of-america-technology-spending/>.

⁴ See Matthew Macia, *Small Banks and the Technology Problem*, Financial Tech Review, <https://www.financialtechreview.com/cxinsight/small-banks-and-the-technology-problem-nwid-16.html> (last visited on Feb. 3, 2021).

⁵ <https://plaid.com/blog/introducing-plaid-exchange/>

⁶ <https://plaid.com/blog/plaid-exchange-jack-henry/>

⁷ <https://plaid.com/blog/q2-and-plaid-partner-to-bring-open-finance-to-millions/>

3. The Bureau should monitor practices to ensure competitive incentives do not harm consumer access

The growth of financial technology, powered by consumer-permissioned data sharing, has led to lower costs for consumers, greater inclusivity in financial services,⁸ and a wider range of available products and services to millions of consumers historically left out of the mainstream.⁹ Many of these benefits are a direct result of consumers gaining choices outside the traditional financial institutions, creating a competitive and dynamic ecosystem. Unfortunately, some data holders limit their customer's ability to share data, actions that have the effect — if not the intention — of maintaining a moat that limits consumers ability to shop for services from a competitor.

Consumer advocates and emerging businesses recognize the importance of preventing such anti-competitive practices. In a recent letter to the Bureau, eighteen advocacy groups acknowledged these dynamics at play.¹⁰ According to Economic Liberties' Director of Policy & Advocacy Morgan Harper, "Consolidation in the financial services industry has given big banks inordinate power, especially over a huge amount of consumer data."¹¹ Even when a consumer has expressly requested to share a certain data field necessary for their desired use case, institutions may effectively block this request by placing limits on the type of data shared, how and how often the data is shared, and with whom the consumer can share their data. Currently, consumers have no timely or sufficient remedy under law to ensure they can share their data as they choose.¹² Petal Card, Inc highlighted similar concerns related to small business and consumer data sharing in their response: "In the absence of standardized, reliable data access, Petal faces frequent business interruption related to downtime, brown-outs, missing data fields and institutions that refuse altogether to honor consumer requests for their electronic financial data."¹³

To address these concerns, Congress should encourage the Bureau to monitor practices to ensure competitive incentives do not harm consumer access. Competitive incentives in the authorized access ecosystem will continue to grow as data holders become data users and vice versa.¹⁴ The Bureau should prevent data holders, whether they are financial applications or financial institutions, from restricting consumer data access to further their competitive interests at the cost of consumer benefit.

⁸ <https://plaid.com/blog/the-fintech-effect-consumer-impact-and-a-fairer-financial-system/>

⁹ See Mehrsa Baradaran, *How the Other Half Banks: Exclusion, Exploitation, and the Threat to Democracy* (2015).

¹⁰ https://www.economicliberties.us/wp-content/uploads/2021/05/CFPB-Letter_5.27.pdf

¹¹ *Id.*

¹² See Plaid's Comments, <https://www.regulations.gov/comment/CFPB-2020-0034-0045> (Response to Question 7)

¹³ See Plaid's comments <https://www.regulations.gov/comment/CFPB-2020-0034-0033> (Recommendation 2)

¹⁴ See <https://www.americanbanker.com/opinion/open-banking-must-be-a-two-way-street>

The combination of these measures will enhance transparency for consumers, ensure strong competition and access to affordable financial services, and provide meaningful privacy protections to safeguard data of consumers.



September 17, 2021

The Honorable Stephen Lynch
Chair
Task Force on Financial Technology
2109 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Warren Davidson
Ranking Member
Task Force on Financial Technology
2113 Rayburn House Office Building
Washington, D.C. 20515

Re: Financial Technology Task Force Hearing on "Preserving the Right of Consumers to Access Personal Financial Data"

Dear Chair Lynch and Ranking Member Davidson:

The Clearing House Association and The Clearing House Payments Company¹ (collectively, The Clearing House) appreciate the Financial Technology Task Force's interest in issues relating to consumer access to personal financial data and thank you for this opportunity to submit a statement for the record. The Clearing House and its member banks are fully supportive of and, as more fully detailed in this letter, have engaged in substantial work with other industry stakeholders to facilitate the ability of consumers, upon request, to safely and securely obtain information about their ownership or use of a financial product or service from their product or service provider.

The market for consumer data has evolved significantly since your Task Force held its last hearing on this issue in November of 2019. The Clearing House and its member banks have played a pivotal role in the intervening market developments and write to update the Task Force on those developments as well as important issues that are yet to be resolved.

I. Industry Initiatives

Much of the market's progress has been and continues to be driven through various industry initiatives aimed at migrating the practice of data sharing away from credential-based data access and screen scraping to a safer, more secure, and more consumer-centric API environment. These initiatives are described below.

¹ The Clearing House is a nonpartisan organization that engages in research, analysis, advocacy, and litigation focused on financial regulation that supports a safe, sound, and competitive banking and payments system. The Clearing House Payments Company L.L.C., owns and operates core payments system infrastructure in the U.S. See The Clearing House's web page at: www.theclearinghouse.org

a. The Clearing House's Connected Banking Initiative

The Clearing House's Connected Banking initiative seeks to enable "innovation and customer control through a more secure exchange of financial data."² The initiative recognizes the need to move beyond a system of credential-based data access and screen scraping and to a safer, more secure, more transparent and consumer-centric API environment.

The terms "credential-based data access" and "screen scraping" may sound innocuous, but they are not. Credential-based data access involves consumers sharing their internet banking platform login credentials (user ID and password) with a third party. These are the same login credentials that consumers use to authenticate into their internet banking platform in order to move money and initiate other financial transactions and services. When consumers share their login credentials, FI data holders may not be able to distinguish whether the login credentials are being used by the consumer, an authorized third party, or a fraudster. Indeed, it is interesting to note that some data aggregator and data user agreements reviewed by The Clearing House *prohibit* the data aggregator's or data user's customers from sharing the data aggregator's or data user's internet platform login credentials (provided by the data aggregator or data user) with any third parties, such practice apparently being viewed by data aggregators and data users as a significant risk to their own data security and integrity.³

Similarly, the process of screen scraping also carries significant risks. Screen scraping refers to the practice by which a data aggregator or data user employs automated processes to "scrape" data from the FI data holder website. In most circumstances, this includes far more data than is actually needed to power the product or service being provided, including personally identifiable information or other sensitive information that the consumer may not have authorized if the process were more transparent to – and capable of being controlled by – the consumer. In addition, screen scraping is more prone to inaccuracies and has the potential of creating operational challenges for FI data holders.⁴ In essence, by sharing their credentials

² Detailed information regarding The Clearing House's Connected Banking initiative is available at: <https://www.theclearinghouse.org/connected-banking>.

³ See, for example, Plaid, "End User Privacy Policy," at "Registration" (Feb. 22, 2021) (available at: <https://plaid.com/legal/>) (providing that users "may never share [their] Account information, including [their] Plaid Dashboard password, as well as [their] API authentication credentials, including [their] Client identification Number ('Client ID') and secret, with a third party or allow any other application or service to act as you"); and Robinhood Financial LLC & Robinhood Securities, LLC, "Customer Agreement," at "K. Electronic Access" (June 2020) (available at: <https://cdn.robinhood.com/assets/robinhood/legal/Customer%20Agreement.pdf>) (prohibiting Robinhood users from sharing their usernames, account numbers, and passwords with any third parties).

⁴ Many financial institutions report that a majority of internet traffic on their banking platforms comes not from the financial institution's customers but from data aggregators constantly pinging the site for data. This traffic can crowd out financial institution customer use, disrupt the smooth operation of the banking platform, and mimic denial of service attacks, slowing the platform or bringing it down completely. Kuepper, Justin "Top Problems with

and submitting their accounts to screen scraping, the consumer is relinquishing control over how much data is being shared and is opting into an inherently risky environment. This is why the CFPB in its Principles for Consumer Authorized Data Sharing and Aggregation (Principles) stated directly that access to data should not “require consumers to share their account credentials with third parties.”⁵

APIs offer significant advantages over credential-based data access and screen scraping. As the Consumer Financial Protection Bureau noted in its Taskforce Report:

An API is a structured data feed that connects the account holder, such as the consumer’s bank, to the data aggregator [Note omitted]. Because an API requires an agreement between the account holder and the data aggregator, parties to an API have the opportunity to agree on terms regarding the scope of data that the account holder will provide to the data aggregator, how often the account holder will provide or update that information, limits on the data aggregator’s use or resale of data, and other terms, such as the parties’ respective liabilities to each other and the consumer.

APIs do not require consumers to provide their security credentials to the data aggregator; instead, the consumer can authenticate the aggregator with the financial institution, and the institution will provide an access token to the aggregator. As a result, an API may limit a data aggregator’s access to certain account information or account services, such as making electronic fund transfers.⁶

To facilitate the transition from credential-based access and screen scraping to APIs, The Clearing House is actively engaged in the development of new technology standards, infrastructure, innovative solutions to address risk management requirements and legal agreements, and in ongoing industry collaboration.⁷ The initiative is guided by the goal of acting “in the best interest of consumers [to] enhance safety and foster efficiency in financial services.”⁸

Financial Data Aggregation” (April 5, 2019) (available at: <https://www.investopedia.com/articles/financial-advisors/021216/top-problems-financial-data-aggregation.asp>).

⁵ “Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation,” (October 18, 2017) (available at: https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf).

⁶ CFPB Taskforce Report, Vol 1, pp. 489-490.

⁷ *Id.* The work being done by The Clearing House is specifically acknowledged in the CFPB Taskforce Report. *See, CFPB Taskforce Report*, Vol 1, p. 495, n. 139.

⁸ *Id.*

The Clearing House's Connected Banking initiative has yielded a number of important deliverables:

- API Technical & Security Standards: The Clearing House and many of its member banks are founding members of the Financial Data Exchange (FDX), which was created to be an organization through which cross-industry participants could develop, maintain, and facilitate the adoption of common API standards for sharing consumer financial data.⁹ More detailed information on the work of FDX is provided below.
- Model Agreement: In order to enhance consumer control over the data they share with data aggregators and data users and to provide for a safer and more secure method to facilitate such sharing, the Connected Banking initiative has focused on accelerating the ability of data holders, data aggregators¹⁰ and data users to establish safe and secure direct connections through APIs. Recognizing that legal agreements between data holders and authorized entities¹¹ can take considerable time and resources to develop, The Clearing House, in collaboration with its member banks and in consultation with data aggregators and data users, developed a Model Agreement that can be used as a reference to facilitate the development of API-related data sharing agreements. The Model Agreement was based on a number of already existing bilateral agreements in the market and was specifically developed to be consistent with the CFPB's Principles and focus on consumer control and transparency, safety and security of the data, and

⁹ Additional information on The Clearing House's support for FDX is contained in: The Clearing House, "The Clearing House Supports Financial Data Exchange Work on API Technical Standards" (Oct. 18, 2018) (available at: <https://www.theclearinghouse.org/payment-systems/articles/2018/10/data-privacy-10-18-2018>).

¹⁰ The CFPB has defined "data aggregator" as "an entity that supports data users and/or data holders in enabling authorized data access." *Id.* According to the CFPB's Taskforce on Federal Consumer Financial Law ("Taskforce"), which released a two-volume report on January 5th ("CFPB Taskforce Report") containing recommendations on how to improve consumer protections in the financial marketplace, "there may be at least 120 or as few as a handful of firms that engage in this activity." The CFPB Taskforce Report notes a Vermont law that requires parties that buy or sell third-party data to register with the secretary of state and that as of March 2019, 121 firms had registered. The CFPB Taskforce Report further notes that some of these entities – such as the National Student Clearinghouse and the nationwide consumer reporting agencies – are not typically thought of as data aggregators in the consumer finance market, even though they gather and provide consumer data. "Focusing more narrowly on financial data aggregators," the CFPB Taskforce Report posits that "there are as few as six significant firms in the market." CFPB Taskforce Report, Vol 1, pp. 494-495.

¹¹ The CFPB has defined "authorized entities" as "entities or persons with authorized data access to particular consumer financial data." *Id.*

appropriate accountability for any risks introduced into the system.¹² Bilateral agreements play a vital role in today's data sharing market. In the absence of an over-arching legal framework developed through regulatory action or otherwise, bilateral agreements are, for now, the only way that FI data holders can allocate liability, ensure transparency and consumer control, and address many other fundamental issues.¹³

- **Uniform Assessment Instrument** Meeting regulatory expectations for due diligence on parties with whom an FI data holder is sharing data (either through an API or otherwise) can be significantly burdensome in terms of time and resources committed for both the FI performing the due diligence and the data aggregator or data user on whom due diligence is being performed, with each FI historically performing one-off due diligence inquiries.¹⁴ In order to create efficiencies and encourage the development of API relationships, The Clearing House developed a uniform assessment instrument that is being used in the market today that streamlines due diligence, allowing due diligence information to be collected once by assessment vendors and then shared by assessment vendors with multiple FIs through their secure portal thereby alleviating largely redundant processes across the financial ecosystem.
- **Central Utility Option:** The Clearing House and a number of its member banks played a pivotal role in the spinout of Akoya L.L.C. ("Akoya") from Fidelity Investments, Inc. and the positioning of Akoya to provide an option that solves for connectivity issues in an API-reliant ecosystem. The role Akoya is playing in the market is discussed in more detail below.

¹² More information on the Model Agreement is available at: <https://www.theclearinghouse.org/connected-banking/model-agreement>.

¹³ While bilateral agreements may be needed for some time in the future, it is anticipated that small banks will ultimately be able to leverage bilateral agreements between their third-party service providers and data aggregators and data users. There is also the potential for entities that play a central utility role, like Akoya, to develop common rule sets or agreements that may ultimately take the place of some or all of the content that is covered in bilateral agreements today.

¹⁴ See, for example, OCC, "Third-Party Relationships: Risk Management Guidance," OCC Bulletin 2013-29 (Oct. 30, 2013) (available at: <https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html>), and OCC, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," OCC Bulletin 2020-10 (March 5, 2020) (available at: <https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html>) (FAQ #4, in particular, relates to the application of OCC guidance to data aggregation relationships).

- Consumer Research: The Clearing House's Connected Banking initiative has been further guided by in-depth consumer research on consumer preferences and awareness regarding the data practices of the financial applications they use. Key findings include:
 - Consumers want better education and more control over access to their information;
 - While consumers tend to feel secure about using financial applications, most are unclear about the terms and conditions of the service providers they use;
 - When they learn more about the actual practices of the data users that provide them with the financial applications they use, their trust in data privacy and security is eroded; and
 - Most consumers are not aware of the full range of personal and financial information financial applications have access to, for how long they retain that access, and what actions the application service provider can take with their information.¹⁵

b. FDX

FDX is an international, nonprofit organization operating in the US and Canada that is dedicated to unifying the financial industry around the FDX Application Programming Interface (FDX API), which is a common, interoperable, royalty-free standard for the secure access of permissioned consumer and business financial data. FDX has broad stakeholder representation and is currently comprised of 200 data providers (i.e., financial institutions), data recipients (i.e., third-party financial technology companies or fintechs and financial institutions¹⁶), data access platforms (i.e., data aggregators and other ecosystem utilities), consumer groups, financial industry groups and other permissioned parties in the user-permissioned financial data ecosystem.

FDX exists chiefly to promote, enhance, and seek broad adoption of the FDX API technical standard, which allows for consumers within the financial data ecosystem to be securely authenticated without the sharing or storing of their login credentials with third parties. Broad adoption of the FDX API standard will help to transition the industry away from

¹⁵ See The Clearing House, "Consumer Survey: Financial Apps and Data Privacy," p. 3 (Nov. 2019) (noting that "[m]ost financial app users are not aware of the personal and financial data the apps have access to") (available at: [https://www.theclearinghouse.org/-/media/new/The Clearing House/documents/data-privacy/2019-The Clearing House-consumersurveyreport.pdf](https://www.theclearinghouse.org/-/media/new/The%20Clearing%20House/documents/data-privacy/2019-The%20Clearing%20House-consumersurveyreport.pdf)).

¹⁶ Many FIs are both data holders and data users.

screen scraping (the retrieval of financial account information with a user's provided login credentials) and enhances the security and reliability of the flow of user-permissioned data between data holders, data aggregators, and data users. Moving the industry to API based access is important for a number of reasons. Most importantly, the use of credential-based access and screen scraping requires the sharing of sensitive consumer login credentials and provides limited consumer control over the amount of data consumers share with data aggregators and data users. Credential-based access and screen scraping are also inefficient and can place stress on financial institutions due to the sheer number of automated logins. Consumers and financial institutions also incur significant risks associated with potential data breaches at data aggregators and data users and the potential for losses attendant to login credentials and other sensitive consumer information coming into the possession of fraudsters.

The FDX API technical standard seeks to replace the practice of credential-based data access and screen scraping with tokenized access in concert with API-based data collection, which allows a consumer to be securely authenticated at their own financial institution and permission only the data that the consumer would like to share. APIs provide the ability for the consumer to choose the type of data that is shared, with whom, for how long and for what purpose. A standardized API along with other standards that have either been or are being created by FDX (such as authentication, authorization, certification, user experience and consent guidelines) create efficiencies in the ecosystem that help speed the adoption of API based data sharing. Without the FDX standards, the ecosystem would remain fragmented – using incompatible APIs, process and definitions. As a result of the development of the FDX API, over 22 million U.S. and Canadian consumers have already been transitioned away from screen scraping to a version of the FDX API.

In a little over two years, FDX has delivered key standards, guidelines, and best practices into the marketplace. The following are the key FDX deliverables to date and those anticipated in the near future:

- FDX API Specification: Currently at version 4.6, the FDX API offers the ability to access over 620 different financial data elements, including banking, tax, insurance, and investment data, making it one of the most comprehensive Open Finance standards in the world. The FDX API utilizes foundational and globally interoperable standards for security, authentication, data transfer, authorization, API architecture, and identity and represents a global best-in-class solution set for user-permissioned data sharing.
- User Experience & Consent Guidelines: The User Experience and Consent Guidelines are intended to accelerate design decision-making during implementation of data sharing experiences. The guidelines specify what information and control must be given to

consumers to ensure consistent data sharing experience regardless of where their data is held or who they are seeking to share it with.

- Taxonomy of Permissioned Data Sharing: In an effort to align industry stakeholders and help regulators and policymakers better understand and define the various roles and perspectives within the user-permissioned financial data ecosystem, FDX maintains a set of common terminology to be used as a taxonomy for the ecosystem. This documentation also includes a conceptual flow model to show how consumers interact with different participants within the current ecosystem that is evolving from legacy to new technology.
- Use Cases: Use cases are consumer-permissioned scenarios that help users minimize the amount of data they share by defining only the data elements that are needed for a given product or service. FDX use cases allow the financial services ecosystem to identify appropriately circumscribed and certifiable data sets needed to power an application and then utilize an industry-led standard like the FDX API to deploy and increase adoption of these use cases. So far, FDX has approved a Personal Financial Management (PFM) use case and expects to add additional use cases in the future, including credit decisioning, money movement setup and fraud monitoring.
- Developing a Certification Program: A qualification and certification program is needed to ensure common implementation and interoperability of any technical standard. Products (i.e., programs and applications that leverage consumer-permissioned financial data sharing) can be approved by a certification program to test the technical compatibility/interoperability, prior to being marketed as a compliant product, or getting access to certain intellectual property rights. Work continues on FDX's certification platform, and FDX recently released foundational requirements covering availability, performance, and security that implementations of the specification must meet to apply for a FDX use case certification.
- Global Registry: FDX envisions the creation of a registry of trusted organizations in order to help the user-permissioned financial data marketplace clearly identify ever-evolving technologies and new market entrants, as well as the web of often proprietary, incomplete, and incompatible technical standards that complicate the market today. Such a registry will enable those operating within the FDX ecosystem and other

ecosystems to reliably identify and verify trusted organizations. In addition, FDX envisions that the registry will provide assurance regarding reliability and performance of data, traceability, transparency and trust in the FDX certification. FDX intends the Global Registry to act as a non-profit, non-commercial, technology agnostic, multi-tenant, cross-sector, international resource.

The work being done by FDX has the benefit of further enhancing competition and innovation in financial services. A common, interoperable, royalty-free, market-led standard that has broad stakeholder support imposes foundational requirements for entities seeking to serve the market for user-permissioned data sharing. Further, FDX as a non-profit industry standards body also provides large incumbents and small start-ups alike with a level playing field on which to compete.

c. Akoya

While the development of API standards such as those developed by FDX plays a critical role, standards still need to be implemented through actual API connectivity. Without the creation of a central utility, each data holder needs to establish individual connectivity with each data aggregator or data user. This one-to-one model, which would require a plethora of individual and potentially differently configured connections across the ecosystem, can be made more efficient for data aggregators, data users and data providers alike. Akoya provides an option that solves for the inefficiencies of this model by providing a one-to-many architecture, in which each data holder can reach any Akoya connected data aggregator or data user through a single API connection with the central utility, Akoya. Data aggregators, data users and data holders alike all have the opportunity to benefit from only integrating once with the Akoya Data Access Network in order to be able to securely exchange consumer-permissioned financial data with one another. The efficiency offered to the market by Akoya may be particularly beneficial to smaller financial institutions and their third-party service providers as they seek to implement API-based data sharing capabilities.

In addition, Akoya facilitates the control, transparency, safety and security that are needed in the data aggregation space. Consumers using Akoya never disclose their user names and passwords (or login credentials) and instead log in directly with their data holder to authenticate and then grant access to a data aggregator or data user. Further, Akoya is fully compliant with the FDX API specification and does not retain any of the data that passes through the network. Members of the Akoya Data Access Network receive web applications that provide documentation, reports and information on data elements that are being accessed and the products that are accessing them. Consumers can review, update, and revoke data access to their authorized entities through an interface provided within their existing digital

The Honorable Stephen Lynch
The Honorable Warren Davidson

-10-

September 17, 2021

experience at the FI data holder.¹⁷ These qualities allow Akoya to serve as a model reference for how the consumer permissioned data access can be implemented in a manner that puts consumer interests at the forefront.

II. Regulatory Activities

In addition to industry activities, the federal financial regulatory agencies have also proposed taking various actions relating to consumer data access.

a. CFPB ANPR on Consumer Data Access

In October of 2020, the CFPB issued an Advanced Notice of Proposed Rulemaking (ANPR) on “Consumer Access to Financial Records”¹⁸ through which the CFPB solicited comments and information to assist the CFPB in developing regulations to implement Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act.¹⁹ The Clearing House notes that the CFPB has engaged in considerable prior work in this area, including a previous Request for Information on *Consumer Access to Financial Records* in November of 2016²⁰, the release of the Principles in October of 2017²¹ and, more recently, arranging a symposium on *Consumer Access to Financial Records* in February of 2020.²² The CFPB has taken a cautious and thoughtful approach to issues relating to data access, which we appreciate, especially given the complexity of the subject matter. A summary of the recommendations The Clearing House submitted to the CFPB in response to the ANPR is set forth in Appendix A to this statement.²³

While the CFPB may issue an actual rule in the future, the CFPB’s most important work to date on issues relating to Section 1033 has been the development and release of the Principles in October of 2017. The Principles, which took into consideration feedback provided by a wide range of stakeholders in response to the CFPB’s prior RFI, set forth the CFPB’s vision for how consumers should be protected when they authorize third party companies to access

¹⁷ Additional information about Akoya and the Akoya Data Access Network is available at: <https://akoya.com/>.

¹⁸ Consumer Access to Financial Records, 85 Fed. Reg. 71,003 (Nov. 6, 2020).

¹⁹ See 12 U.S.C. § 5533.

²⁰ Request for Information Regarding Consumer Access to Financial Records, 81 Fed. Reg. 83,806 (Nov. 22, 2016).

²¹ Consumer Financial Protection Bureau, “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).

²² See Consumer Financial Protection Bureau, “Bureau Symposium: Consumer Access to Financial Records, a summary of the proceedings” (July 24, 2020) (summarizing the Bureau’s symposium) (available at: <https://www.consumerfinance.gov/data-research/research-reports/bureau-symposium-consumer-access-financial-records-summary-proceedings/>).

²³ A copy of The Clearing House’s comment letter is available at: <https://www.theclearinghouse.org/advocacy/articles/2021/01/consumer-access-financial-records-02-04-2021>.

their financial data to provide certain financial products and services.²⁴ The Principles were “intended to help foster the development of innovative financial products and services, increase competition in financial markets, and empower consumers to take greater control of their financial lives.”²⁵ TCH and its member banks strongly support the Principles, which have guided our work and that of other industry stakeholders as we have sought to implement the CFPB’s vision, and they remain highly relevant today. Since their release in 2017, much has been accomplished by the industry as it has worked towards making the CFPB’s vision a reality, driven by a shared desire to protect consumers and the safety and security of the financial services ecosystem as the market for services using consumer-authorized financial data continues to develop.

One important concept set forth in the Principles is data minimization. As the CFPB’s Principles note, “[t]hird parties with authorized access [should] only access the data necessary to provide the product(s) or service(s) selected by the consumer.”²⁶ In other words, data aggregators and data users should only access the specific data that is needed, solely for the purpose intended, and should retain the data only for as long as it is relevant to the benefit that was sought by the consumer. Many of the practices prevalent in today’s marketplace unfortunately go well beyond the scope outlined by the CFPB and as a result of more data being beyond harvested than what is needed, risks to consumers and to the financial services ecosystem are unnecessarily increased.

While the Principles have been a useful tool in guiding the industry’s work and much has been accomplished in reliance on them, there are areas, as discussed more fully below, where further action by the CFPB would be useful. In order to continue the industry’s momentum, however, it is imperative that any further action taken by the CFPB be consistent with the CFPB’s prior positions articulated in the Principles and be coordinated with other federal financial services regulators to ensure a consistent approach to issues relating to consumer-permissioned data access. Such a consistent approach is essential to avoid bifurcating the market, which could greatly inhibit the scalability of industry standards, utilities, and other solutions.

²⁴ Consumer Financial Protection Bureau, “CFPB Outlines Principles For Consumer-Authorized Financial Data Sharing and Aggregation” (Oct. 18, 2017) (available at: <https://www.consumerfinance.gov/about-us/newsroom/cfpb-outlines-principles-consumer-authorized-financial-data-sharing-and-aggregation/>).

²⁵ *Id.*

²⁶ “Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation,” (October 18, 2017) (available at: https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf).

b. Joint Agency Proposal on Third Party Risk Management Guidance

At the same time that the CFPB is undertaking a rulemaking to more fully implement the provisions of Section 1033, the Federal Deposit Insurance Corporation (FDIC), Board of Governors of the Federal Reserve System (Fed), and the Office of the Comptroller of the Currency (OCC) are engaged in a rulemaking that would create uniform guidance on third-party risk management across the spectrum of financial institutions that are subject to the regulation and supervision of these agencies.²⁷ The proposed guidance is intended to assist FIs in managing third-party relationships, including addressing “consumer protection, information security, and other operational risks.”²⁸ Data aggregator relationships are amongst those third-party relationships that are covered by the Proposal, which appropriately emphasizes both the need to protect the FI and the FIs’ customers given the risks that are inherent in these kinds of relationships.²⁹

The standards and requirements set forth by the agencies in the proposed guidance, which emphasize FI responsibility for safety, soundness, and consumer protection, and the standards and requirements to be set forth by the CFPB, which will undoubtedly emphasize data access, run the risk of being inconsistent. Absent coordination amongst the agencies and the CFPB to create a unified framework for third-party risk management and data access as it relates to data aggregation activities, FIs may well be caught between two competing sets of regulatory expectations.

This is due in no small part because the tools that banks have to address safety and soundness and consumer protection risks associated with data aggregators are at best blunt instruments. First, all but perhaps the biggest banks with the richest troves of data lack the degree of negotiating power that would be needed to impose the kinds of safety and soundness and consumer protection requirements that the proposed guidance outlines. The status quo – credential-based data access and screen scraping – is always a potential fall-back for any data aggregator that doesn’t want to adhere to the kinds of structure and requirements that sound third-party risk management practices may impose. FI control is even more attenuated when it comes to data aggregator clients, or “fourth parties” who could be considered “subcontractors” under the proposed guidance and therefore subject to some degree of third-party risk management activities by the affected FI.³⁰ There may be thousands of fourth party data recipients that receive data from a particular data aggregator. The

²⁷ “Proposed Interagency Guidance on Third-Party Relationships: Risk Management,” 86 FR 38182 (July 19, 2021).

²⁸ 86 FR 38184

²⁹ “Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29,” *supra* note 14, at Frequently Asked Question #4.

³⁰ 85 FR 71005 - 71006.

identities of these fourth parties are seldom disclosed to FIs and, even if disclosed, the ability of FIs to do third-party risk management due diligence on all of them is a practical impossibility.

Second, FIs whose systems are being targeted with credential-based data access and screen scraping from data aggregators that do not or will not comply with reasonable risk-management controls and requirements will likely face a Cornelian dilemma of either continuing to allow the data aggregator to have access to the bank's systems or cutting off the data aggregator's access until such controls can be put in place. In the first instance, the bank may risk exceeding its own risk tolerance, potentially running afoul of regulatory expectations and seeing its business, systems, and customers harmed. In the second instance, the bank risks upsetting its own customers who may not understand the bank's actions as being motivated by the banks' desire to ensure their protection and the bank may suffer reputational harm as a result.³¹

Finally, while an FI may attempt to exclude a non-compliant data aggregator by blocking its IP address, that action provides only a temporary solution. Nothing prevents the data aggregator from obtaining a new IP address from which the data aggregator can then seek renewed access to the FI's systems. FIs also face the practical reality that technology is always evolving and regardless of actions taken by an FI to block a non-compliant data aggregator, data aggregators and fintechs will always have a vested interest in obtaining the data, which is the lifeblood of their business.

To be able to ensure that data access is occurring in a safe and sound manner consistent with the proposed guidance, FIs must have the ability to prohibit credential-based access and screen scraping once an FI is providing data access through an API on fair and reasonable terms. Further, to ensure that the industry as a whole transitions to APIs and that risks to the ecosystem are being appropriately managed, The Clearing House encourages the agencies to

³¹ Data aggregators have been quick to portray such bank actions as anticompetitive and motivated by considerations other than sound third-party risk management. For example, JPMorgan Chase (JPMC) is working towards imposing stricter security standards that will result in JPMC's customers' passwords getting "out of the system," by requiring secure tokens to be used by third parties such as aggregators, resulting in a safer and more secure data sharing environment. Actions like the one being taken by JPMC, however, have sometimes been portrayed as controlling and threatening by technology company executives and Silicon Valley. (See Laura Noonan, "JPMorgan to ban fintech apps from using customer passwords," Financial Times (Jan. 2, 2020) (available at: <https://www.ft.com/content/93dcfc52-210b-11ea-b8a1-584213ee7b2b>) (noting that JPMC is moving to implement more robust security standards, and quoting Bill Wallace, JPMC's head of digital, about the importance of removing customer passwords from systems); and Jennifer Surane, "Big Banks' Clampdown on Data Puts Silicon Valley Apps on Alert," Bloomberg (March 26, 2019) (available at: <https://www.bloomberg.com/news/articles/2019-03-26/jpmorgan-s-clampdown-on-data-puts-silicon-valley-apps-on-alert>) (noting that a number of Silicon Valley ventures say they've been threatened by banks' implementation of security measures).

consider establishing a definitive end to credential-based access and screen scraping, which could be phased in based on the size of the institution.³²

The agencies need to work together to develop a unified framework that not only provides for data access, but empowers FIs to establish the kinds of controls and mitigate the kinds of risks covered by the proposed guidance. The Clearing House believes that this must include ultimately addressing the risks associated with credential-based access and screen scraping by ending such practices once an FI has made API access available on fair and reasonable terms. The Clearing House further believes that the development of a unified framework can only be achieved through strong coordination amongst the FDIC, Fed, OCC and CFPB.

c. The need to clarify application of the Gramm Leach Bliley Act to data aggregators and to ensure that there is a regulatory and supervisory framework in place that imposes standards and supervision on data aggregators that is commensurate with the standards imposed on FIs when FIs are handling similar customer information.

Empowering the actions noted above will be helpful, but, in the absence of a robust regulatory and supervisory framework that imposes meaningful standards and supervision on data aggregators, it will still be inadequate. Banks cannot and should not be expected to shoulder the burden of policing an entire industry, particularly where the data aggregator is not a third-party vendor to the bank and the bank's only connection with the data aggregator is a result of the bank working to accommodate its customer's desire for data to be made available. Further, not all FI data holders have the wherewithal to perform due diligence and impose controls on data aggregators and, more importantly, no FI, regardless of size, will be able to address security practices at the thousands of fintech data users that comprise data aggregator clients. While FIs may attempt to address security issues in bilateral agreements, such agreements must be individually negotiated and data aggregators have a powerful default position to simply continue credential-based access and screen scraping if the FI attempts to impose requirements that the data aggregator does not wish to incorporate.

³² The agencies have successfully set target dates to meet regulatory expectations in other areas, successfully transitioning the industry away from practices that did not meet regulatory expectations. For example, the Federal Reserve, FDIC, and OCC jointly issued a statement on banks' transition away from USD LIBOR that, as part of an orderly, safe, and sound transition away from use of the rate due to regulatory concerns, encourages banks to cease entering into new contracts that use USD LIBOR as a reference rate as soon as practicable, but, in any event, to cease entering into such contracts by December 31, 2021. (See Federal Reserve, FDIC, OCC, "Statement on LIBOR Transition" (Nov. 30, 2020) (available at: <https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201130a1.pdf>.)

The proposed guidance on third-party risk management promulgated by the FDIC, Fed and OCC notes that a “key focus” of an FI’s risk management activities relating to data aggregators should be on information security. This issue, however, can and should be more directly addressed by ensuring that data aggregators are subject to a meaningful regulatory framework, including supervision for information security practices.

Federally chartered banks are subject to detailed Federal Financial Institutions Examinations Council (FFIEC) guidance on information security and the interagency rules implementing the Gramm Leach Bliley Act (GLBA) and, more importantly, supervision and enforcement by the Federal financial regulatory authorities. Even state-chartered FIs are required to comply with detailed security measures and are subject to state regulatory supervision and enforcement actions. Those regulatory frameworks are key to protecting consumers and preventing data breaches, transmission errors, unauthorized access, and fraud, all of which are fundamental concerns that go to the heart of data sharing activities. Data aggregators and fintech data users that sit underneath them, on the other hand, are, *at most*, subject to the much less stringent FTC safeguards rule and, in most instances, no regulatory supervision and only after the fact enforcement by the FTC.³³ Yet even application of the much weaker standards in the FTC’s safeguards rule to data aggregators is in doubt. As the CFPB has noted, “there may be some uncertainty about whether a data aggregator is a ‘financial institution’ subject to [GLBA] and [the] Privacy and Safeguards Rules.”³⁴ Effective information security protection should *begin* with the FTC ensuring that there is *no room for ambiguity* as to whether GLBA applies to data aggregators and fintech data users. Consumers deserve no less protection.

In addition, the FTC must ensure that the safeguards rule is strengthened as it applies to data aggregators and their fintech clients. While the disparities between the FTC’s safeguards rule and FFIEC standards are legion, a single example may be illustrative. Entities that *are* subject to the FTC’s safeguards rule are *not even required* to have an incident response plan. This means that even if GLBA application to data aggregators and fintech data users is clarified, a data aggregator or fintech that is engaged in the business of handling potentially millions of customers’ sensitive, personal financial data is not required under the FTC’s safeguards rule to have *any* plan in place to respond to an information security incident, such as a widespread

³³ See FTC, “Standards for Safeguarding Customer Information” (codified at 16 C.F.R. Part 314) (notably, the FTC safeguards rule contains general requirements that are less detailed than the requirements provided under the Gramm-Leach-Bliley Act (differences between the two sets of requirements include standards regarding board and management involvement, employee background checks, vendor oversight, authentication, and incident response programs)). See also 81 FR 61632 (Sept. 7, 2016) (requesting public comments on the standards for safeguarding customer information, including comment on whether a response plan should be a required element of an information security program).

³⁴ “Taskforce on Federal Consumer Financial Law Report[.] Vol. 1,” *supra* note 7, pp. 513-514.

data breach. While the FTC began work in 2016 to modernize the safeguards rule, that work was never completed.³⁵ An updated standard is needed the FTC should complete its work to modernize the safeguards rule so that meaningful consumer protection is provided and standards are imposed that are equivalent to those imposed on FIs when handling similar information.

Regulatory standards alone, however, are not sufficient without meaningful supervision and enforcement.³⁶ Accordingly, the CFPB must ensure that it incorporates a meaningful supervisory framework in the context of its rulemaking under Section 1033.³⁷ The security of consumer data has been the subject of considerable concern by Congress and others, which

³⁵ In the meantime, data aggregation and fintech users have multiplied exponentially. 54% of U.S. banking consumers use financial apps to engage in personal financial management, investing, borrowing, and person-to-person payments; the aggregation system is thought to reach approximately 95% of U.S. deposit accounts; and one large aggregator in the U.S. estimates that it alone connects to one in four financial accounts in the U.S. (See “Consumer Survey: Financial Apps and Data Privacy,” *supra* note 11, pp. 2 & 4; Michael Deleon, “A buyer’s guide to data aggregation,” *Tearsheet* (Feb. 19, 2019) (available at: <https://tearsheet.co/data/a-buyers-guide-for-data-aggregation/>); and Zack Meredith & Zeya Yang, “The all-new Plaid Link,” *Plaid Blog* (Oct. 2, 2020) (available at: <https://plaid.com/blog/the-all-new-plaid-link/>)). Additionally, the COVID-19 pandemic appears to be playing a role in accelerating U.S. consumers’ adoption of fintech applications, with older generations in particular using fintech applications in increasing numbers. (See Krivkovich, White, Townsend & Euart, “How US customers’ attitudes to fintech are shifting during the pandemic,” McKinsey & Company (2020) (available at: <https://www.mckinsey.com/industries/financial-services/our-insights/how-us-customers-attitudes-to-fintech-are-shifting-during-the-pandemic>)).

³⁶ The FTC, for example, has limited supervision and enforcement powers. See FTC, “A Brief Overview of the Federal Trade Commission’s Investigative, Law Enforcement, and Rulemaking Authority,” FTC memorandum (May 2021) (available at: <https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority>). See also “Prepared Statement of the Federal Trade Commission: Strengthening the Federal Trade Commission’s Authority to Protect Consumers” (Apr. 20, 2021) (available at: https://www.ftc.gov/system/files/documents/public_statements/1589164/prepared_statement_of_the_ftc_before_the_senate_committee_on_commerce_science_and_transportation.pdf); and “Prepared Statement of the Federal Trade Commission: The Urgent Need to Fix Section 13(b) of the FTC Act” (Apr. 27, 2021) (available at: https://www.ftc.gov/system/files/documents/public_statements/1589400/p180500house13btestimony04272021.pdf) (noting that the FTC lacks authority and requesting that Congress act to clarify Section 13(b) of the FTC Act so as to preserve / strengthen the FTC’s ability to enjoin illegal conduct). As we have seen from the 2017 Equifax data breach that exposed the personal information of 147 million people, the extensive risks to consumers who are victims of a data breach cannot be effectively remedied by an after-the-fact civil money penalty. Proactive examination and, where necessary, remedial action are the most effective tools to help prevent consumer harm from occurring in the first place.

³⁷ The CFPB could also use its rulemaking power to impose meaningful information security standards on data aggregators and their fintech clients in the absence of FTC action on the safeguards rule. See CFPB, “Rules and policy” (available at: <https://www.consumerfinance.gov/rules-policy/>) (noting that the CFPB generally has authority to make rules governing consumer finance markets and that it can “create new rules when warranted”). See also Adam J. Levitan, “The Consumer Financial Protection Bureau: An Introduction,” *Review of Banking & Financial Law*, Vol. 32, pp. 344-347 (2012-2013) (available at: <https://www.bu.edu/rbfl/files/2013/10/Levitan.pdf>) (noting ways that the CFPB’s rulemaking authority reaches “covered persons” and “service providers”).

have focused on the perceived misuse of consumer data by numerous fintech companies.³⁸ Similarly, the Facebook/Cambridge Analytica scandal shows that even with appropriate contractual limitations in place, absent robust third-party risk management processes and appropriate supervision and enforcement the security of data cannot be assured.³⁹ In the context of data sharing under Section 1033, the data at issue, dealing with a consumer's financial information and often including PII, is even more sensitive than generalized consumer data and its distribution and use should be subject to heightened concern.

To better ensure the protection of consumers and the FI ecosystem, the CFPB must develop a regulatory and supervisory framework that imposes standards and supervision applicable to data aggregators that is commensurate with the standards and supervision imposed on FIs when FIs are handling similar customer information. Given data aggregator and data user access to similarly sensitive information, data aggregators that are the recipients of such information should be subject to CFPB regulation and supervision that includes functionally similar requirements as those imposed on FIs, including supervision and enforcement that the CFPB should provide through a larger participant rule or otherwise.⁴⁰ In order to ensure a fully secure ecosystem, such requirements should follow the data with data aggregators being responsible for passing on and enforcing security requirements to data users. Further, inherently risky practices such as credential-based access and screen scraping should be phased out, with the federal financial regulators setting a firm target, perhaps phased in by institution size, for such activities to cease.

³⁸ See, for example, NPR, "Amazon, Tik Tok, Facebook, Others Ordered to Explain What they Do With User Data" (Dec. 15, 2020) (available at: <https://www.npr.org/2020/12/15/946583479/amazon-tiktok-facebook-others-ordered-to-explain-what-they-do-with-user-data>); Lauren Feiner, "Big Tech Testifies: Bezos Promises Action if Investigation Reveals Misuse of Seller Data, Zuckerberg Defends Instagram Acquisition," CNBC (Sept. 8, 2020) (available at: <https://www.cnbc.com/2020/07/29/tech-ceo-antitrust-hearing-live-updates.html>); Elizabeth Dwoskin, "Facebook is Accused of Digital 'Surveillance' Against Its Competitors," The Washington Post (July 29, 2020); and Michael Grothaus, "How Our Data Got Hacked, Scandalized, and Abused in 2018," Fast Company (Dec. 13, 2018) (available at: <https://www.fastcompany.com/90272858/how-our-data-got-hacked-scandalized-and-abused-in-2018>).

³⁹ See Nicholas Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far," The New York Times (April 4, 2018) (available at: <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>); and Paolo Zialcita, "Facebook Pays \$643,000 Fine For Role In Cambridge Analytica Scandal," NPR (Oct. 30, 2019) (available at: <https://www.npr.org/2019/10/30/774749376/facebook-pays-643-000-fine-for-role-in-cambridge-analytica-scandal>).

⁴⁰ Such supervision would necessarily include supervision over the data aggregators' third party risk management program pursuant to which the data aggregator would be responsible for evaluating and managing risks associated with its data user customer's use of consumer data.

d. The need to address liability

A fundamental component of the regulatory framework for data aggregators and data users must include provisions that address liability. Data aggregators and data users may have little incentive to end credential-based access and screen scraping without a regulatory mandate to do so. The risks of credential-based access and screen scraping are largely borne by consumers and FI data holders. Existing terms and conditions imposed by data aggregators largely disclaim all or most responsibility for any loss that may result from data aggregator or data user activities. To the extent not accepted by data aggregators and data users, losses will be borne either by consumers or data holders. Consumers bear risks related to misuse of their data and data breaches, including identity theft, breach of privacy, and fraud. FI data holders hold the majority, if not all, of the liability that would accrue from a data breach or the unauthorized use of consumer data, including all of the cost of recredentialing the consumer to prevent further losses and potential liability for unauthorized transfers. Absent further regulatory action, data aggregators may opt to continue the status quo, particularly when one considers the costs of moving to an API environment, including submission to appropriate due diligence, the cost of connectivity, and the fact that the data that will be made available through APIs will be more narrowly tailored to appropriate use. Yet, as noted above, the industry's transition to APIs is fundamental to achieving much of the vision for consumer protection, including enhanced safety, security, transparency and control over data usage.

The Clearing House believes that any future CFPB rulemaking on data access must address liability. The CFPB should prevent data aggregators and data users from disclaiming liability to either the consumer or the data holder for acts or omissions relating to data while it is in their custody or control. Liability should follow the data and all parties should be fully accountable for its care.

The Honorable Stephen Lynch
The Honorable Warren Davidson

-19-

September 17, 2021

III. Conclusion

While much progress has been made by the industry in building out a safer and more secure ecosystem for sharing consumer permissioned data, significant work remains that will require considerable regulatory coordination and activity. The Clearing House appreciates this opportunity to submit this statement for the record, looks forward to providing input into further regulatory activity to implement the provisions of Section 1033 of the Dodd Frank Act, and would welcome the opportunity to serve as a resource to the Task Force in any future hearings.

Respectfully submitted,

/s/

Robert C. Hunter
Deputy General Counsel & Director of Regulatory and Legislative Affairs



APPENDIX A

**SUMMARY OF THE CLEARING HOUSE'S RECOMMENDATIONS TO THE CFPB IN RESPONSE TO THE
CFPB'S OCTOBER 2020 ANPR ON CONSUMER DATA ACCESS**

1. Further guidance consistent with the Principles may be preferable to a rulemaking given the complexity, time and resource commitment required by the CFPB to engage in a successful rulemaking and the potential for delay and uncertainty to freeze progress that the market has been making;
2. The CFPB should continue to rely on private sector market-led efforts for technical standard setting of the kind engaged in by FDX and believes it would be a mistake for the CFPB to attempt to define technical standards. There are a number of actions that the CFPB could nonetheless take that would be consistent with the CFPB's charge in Section 1033 to "promote" the development and use of standardized formats for information. These include:
 - a. Finding ways to explicitly endorse or reference technical standards and certification organizations like FDX and the work that they are doing,
 - b. Providing greater regulatory clarity on the issues discussed below and thereby allowing the industry to then work together to develop or further enhance existing standards to implement the CFPB's vision, and
 - c. Working with other regulators to ensure that the Federal financial regulators are speaking with one voice on issues affecting the data aggregation market.
3. If the CFPB is determined to proceed with a rulemaking, the rulemaking must be holistic in its approach and, at a minimum, address the following issues that are discussed more fully below:
 - a. Credential sharing and credential storage as well as screen scraping pose significant risks to consumers, including risks related to data breaches and fraudulent and unauthorized transfers as well as identity theft and other data privacy issues, and should be abolished as a fundamental part of any rulemaking. Such action could take the form of the CFPB articulating a rule that prohibits a data aggregator or data user from obtaining consumer data using a consumer's online banking credential and screen scraping where a data holder has provided the data aggregator or data user with the option of enabling safer, more secure methods, such as API access under fair and reasonable terms. The CFPB may also wish to consider a rule that sunsets credential-based data sharing, storage and screen scraping upon a schedule that would be phased in over time by institutional size.
 - b. The CFPB in any rulemaking should clarify that data access is limited to circumstances in which a data user will provide services to the consumer that is providing the data, reasonably requires the data to provide those services and does so in a way that is transparent and consistent with consumer expectations. If data is sold to third parties for use in research or analytics unrelated to the underlying service, that information should be clearly and conspicuously disclosed to consumers and subject to their consent.
 - c. The CFPB in any rulemaking should develop disclosure requirements for all parties, including model disclosures that create a safe harbor for various



stakeholders. Requirements must recognize that FI data holders will have limited visibility into data usage and downstream parties. Accordingly, data holders should generally be limited to disclosing to whom the data is initially being provided, the fact that the provision of data was authorized, and identification of the appropriate mechanism through which the consumer may halt the ongoing provision of data. Data aggregators and data users should be required to disclose to consumers the identity of each data user to which the consumer's data is being provided and each data user with whom information is shared should be required to obtain separate and distinct authorization from the consumer for the use of the consumer's data. Disclosure should include what data is being accessing, how frequently it is being accessed, for what purpose, and for how long it is being stored. Disclosures must be sufficiently clear and easily understood by consumers to ensure that authorization is knowingly given with mandatory periodic affirmative reauthorization no less frequently than annually. Disclosures should also clearly spell out the consumer's right to revoke authorization and should include the right to be forgotten. The CFPB should impose a heightened "clear and conspicuous" standard for consent relating to the sale of consumer data unrelated to the direct provision of any service to the consumer.

- d. The CFPB in any rulemaking should clarify that the concept of a "trusted third party" recipient of data requires trust not only by the consumer, but also requires that the data aggregators and data users will have satisfactorily met the FI data holder's own reasonable risk management criteria in order to qualify to receive the data. Given the risks that data aggregators and data users introduce into the ecosystem, such requirements should include not only appropriate information security controls, but also insurance and financial requirements that are commensurate to the risks being introduced.
- e. Regardless of the requirements of any technical standard being applied, the CFPB in any rulemaking should clarify that the standard must be subservient to an overall data minimization principle – that a data aggregator or data user should still only obtain and use data strictly as needed for the service currently being provided, and, further, that the consumer should be fully in control of what categories of data are being provided, to whom, for how long, and for what purpose regardless of use case.
- f. The CFPB in any rulemaking should clarify the nature and extent to which confidential information may be protected from disclosure and should specifically extend the protection for confidential information to commercially sensitive trade secrets that are not otherwise disclosed to consumers. Similar to the prohibitions on reverse engineering that are found in most data aggregator and data user agreements, the protection for confidential information should include a prohibition on the reverse engineering of proprietary algorithms and other processes that are not otherwise disclosed to consumers.
- g. The CFPB in any rulemaking should clarify that FI data holders, who are mere conduits for information being pulled by data aggregators and data users acting as agents for FI data holder customers, are not "furnishers" for purposes of the Fair Credit Reporting Act.



- h. The CFPB in any rulemaking should recognize that the use of data to facilitate the movement of money carries heightened risks for consumers and for FI data holders relating to unauthorized payments and fraud and should affirm the legitimacy of FI data holders imposing reasonable, heightened requirements for the disclosure of information that can be used to initiate payments, including the imposition of enhanced security measures such as tokenization, enhanced due diligence, and enhanced information security controls.
- i. In order to ensure that sensitive consumer financial information is appropriately protected throughout the data lifecycle, the CFPB in any rulemaking should subject data aggregators that are the recipients of such data to functionally similar requirements to those imposed on FI data holders when handling the same information. Data aggregators should also be subject to supervision and enforcement to ensure compliance and should be responsible for passing on and enforcing security requirements to data users.
- j. The CFPB in any rulemaking should recognize and affirm the legitimate role that FI data holders play in protecting their customers and the financial system and should affirm an FI data holder's FI's ability to control access, affirm authentication and impose reasonable time, place and manner restrictions in circumstances that are consistent with protecting the consumer and the safety and soundness of the financial system. This should include any circumstances in which the FI has a good faith belief that access may be fraudulent, may present security risks to the consumer, the FI or the financial system generally, may relate to misuse of the consumer's data or may relate to data beyond that which is reasonably related to the product or service being provided to the consumer or as reasonably needed to protect the security, efficiency and operational integrity of the FI data holder's own systems
- k. The CFPB in any rulemaking should make allowance for FIs to obtain data usage information from data aggregators and data users so that they may voluntarily provide it to consumers if the FI has the ability to provide the consumer with a one-stop, aggregated view of the consumer's data usage. Such an aggregated view is clearly beneficial to consumers and should be encouraged by the CFPB where possible in order to help the consumer be an active participant in stewarding their data.
- l. The CFPB in any rulemaking should interpret the need for data accuracy consistent with data holders making available information that is subject to an FI data holders standard posting times and other procedures that the FI has adopted for data handling in the ordinary course of its business, which is the standard imposed by Section 1033. The CFPB should recognize that FI data holders will have limited understanding and control over downstream uses of data and therefore cannot be guarantors that data accessed will be accurate and current for all purposes and in all circumstances.
- m. FI data holders are already subject to robust regulations and requirements relating to addressing claims of unauthorized access and other consumer disputes and have substantial resources and processes in place to address such issues. Data aggregators and many data users, however, do not. Accordingly, any rulemaking engaged in by the CFPB should adopt a dispute resolution



infrastructure outlining minimum standards for data aggregators and data users commensurate with those already imposed on FI data holders.

- n. Any rulemaking engaged in by the CFPB should prohibit data aggregators and data users from disclaiming liability to either the consumer or the data holder for acts or omissions relating to data while it is in their custody or control, which is today a common practice. Liability should follow the data and all parties should be fully accountable for its care.
- o. In order to ensure that consumers are protected and that there is an appropriate trust environment for the sharing of data, any rulemaking by the CFPB should include an assertion of the CFPB's authority under Section 1024(a)(1)(B) or Section 1024(a)(1)(c) of the Dodd Frank Act and allow for the appropriate supervision and examination of data aggregators with appropriate requirements for data aggregator due diligence and oversight of data users with whom consumer information is shared. FI data holders are already subject to robust supervision and enforcement. Supervision and enforcement of data aggregators is a fundamental component that would be needed to ensure meaningful compliance with any rules developed by the CFPB.
- p. The CFPB should study and evaluate the requirements set forth in Regulation E, which predate the substantial changes that have taken place in the marketplace and that have been facilitated by data aggregation and other activities. Data aggregation activities are increasingly being leveraged to enable payment initiation. Those services frequently exist outside of the control of FI data holders and yet liability for unauthorized transfers and the costs of recredentialing continue to rest with them. Incentives may need realignment to ensure that parties are properly incented to properly protect the data that is in their care.

**Chi Chi Wu Answers to
Williams (GA) Question for the Record
Task Force on Financial Technology Hearing
“Preserving the Right of Consumers to Access Personal Financial Data”
Tuesday, September 21, 2021 at 10:00 a.m.**

Ms. Wu, in your testimony, you mentioned that Black consumers are disparately impacted by bank overdraft practices and that we should keep this in mind when related consumer data is employed.

1a. How could greater use of no-fee accounts address the underlying disparity informing the data going forward?

Accounts that do not permit overdrafts, or “safe accounts,” are one tool that can help reduce the harm caused by unfair overdraft practices. The Bank On initiative has worked with banks to offer and develop safe accounts, which do not charge overdraft and NSF fees and have low monthly maintenance fees.¹ Since Black consumers bear a disproportionate burden from overdraft fees, safe accounts could help lessen this disparity by enabling consumers to avoid such fees.

More importantly, safe accounts could help bring consumers without bank accounts into the banking system. A significant portion of unbanked consumers leave or are forced out of traditional bank accounts because of high overdraft fees.² Black consumers are disproportionately unbanked - 13.8 percent of Black households were unbanked in 2019 (as well as 12.2

¹ Bank On, Bank On National Account Standards (2021 - 2022), <https://2wvkof1mfraz2etgea1p8kiw-wpengine.netdna-ssl.com/wp-content/uploads/2020/10/Bank-On-National-Account-Standards-2021-2022.pdf>.

² Chi Chi Wu and Katie Plat, National Consumer Law Center and Cities for Financial Empowerment Fund, Account Screening Consumer Reporting Agencies: A Banking Access Perspective (Oct. 2015), www.nclc.org/images/pdf/pr-reports/Account-Screening-CRA-Agencies-BankingAccess101915.pdf.

percent of Latinx households) compared to 2.5 percent of white households.³ Being unbanked, of course, excludes consumers from the possibility of using cashflow data. And as stated in my written testimony, when Black consumers do have bank accounts, they bear a disproportionate burden from overdraft fees.⁴

However, safe accounts are just one tool to address the \$11 billion per year drained from consumers' accounts by overdraft fees.⁵ Ultimately, the solution is meaningful reform of unfair overdraft practices, such as prohibiting overdraft fees for ATM and debit card transactions, ensuring that fees are reasonable and proportional, limiting fees to no more than one per month and six per year, and other reforms that consumer advocates have long called for.⁶

Such reforms are also a matter of racial justice. As the Financial Health Network noted in an October 5, 2021 report “Because financial services charges, such as overdraft fees, are disproportionately borne by Black and Latinx consumers, high institutional reliance on overdraft fees risks undermining the commitments many institutions have made to racial equity in recent months.”⁷

1b. Can you tell us the importance of simultaneously addressing concerns with data use and the real-life disparities that inform the data?

³ Federal Deposit Insurance Corporation (FDIC), How America Banks: Household Use of Banking and Financial Services, 2019 FDIC Survey (October 2020), <https://www.fdic.gov/analysis/household-survey/2019report.pdf>, at 2.

⁴ See Pew Charitable Trusts, Heavy Overdrafters, April 2016, <http://www.pewtrusts.org/~media/assets/2016/04/heavyoverdrafters.pdf?la=en>, at 7 (African-Americans are 12 percent of the US population, but account for 19 percent of the heavy overdrafters).

⁵ Peter Smith, Shezal Baba, Rebecca Borne, Center for Responsible Lending, Overdraft Fees: Banks Must Stop Gouging Consumers During the COVID-19 Crisis, June 2020, www.responsiblelending.org/sites/default/files/nodes/files/research-publication/crl-overdraft-covid19-jun2019.pdf.

⁶ *Id.*

⁷ Mark Feldman, David Silberman, Amelia Josephson, Financial Health Network, Reexamining Overdraft Programs: A Guide for Financial Institutions, Sept. 22, 2021, <https://fhn-finhealthnetwork-assets.s3.amazonaws.com/uploads/2021/10/Reexamining-Overdraft-Programs-Report.pdf>.

Traditional credit scores exhibit dramatic racial disparities, as documented by numerous studies.⁸ These disparities are due to a multitude of factors, including the racial wealth gap, decades of redlining and housing segregation, historical and present-day employment discrimination, and racially biased criminal justice practices.⁹

Alternative data has been touted as the solution to this issue, with some arguing that the inclusion of rent, utility, or bank account data will solve the disparities in credit scoring. Indeed, the credit bureaus themselves have heavily promoted the idea of alternative data as a panacea, claiming that it is a form of “credit inclusion.”¹⁰ However, including alternative data in credit reports has the effect of feeding even more of our financial information into the database of these three corporations, increasing their oligopoly power. Consumers need alternatives to the credit bureaus.

Furthermore, while some types of alternative data do hold promise,¹¹ any data that relies on financial information will still reflect racial disparities given the unequal economic positions of households of color and white households. When financially-based data is fed into algorithms or artificial intelligence models, the results could replicate or amplify those disparities.

Researchers have explored methods and tools to reduce these racial disparities, such as the use of adversarial debiasing,¹² and such efforts should

⁸ Chi Chi Wu, National Consumer Law Center, Past Imperfect: How credit scores and other analytics “bake in” past discrimination and perpetuate it, May 2016,

www.nclc.org/images/pdf/credit_discrimination/Past_Perfect050616.pdf.

⁹ Chi Chi Wu, Reparations, Race, and Reputation in Credit: Rethinking the Relationship Between Credit Scores and Reports with Black Communities, Aug. 2020, https://medium.com/@cwu_84767/reparations-race-and-reputation-in-credit-rethinking-the-relationship-between-credit-scores-and-852f70149877.

¹⁰ Consumer Credit Reporting: Assessing Accuracy and Compliance: Hearing Before the Subcomm. on Oversight and Investigations of the H. Fin. Serv. Comm., 117th Congr. (2021) (testimony of John Danaher, President of TransUnion Consumer Interactive) (discussing how “alternative data is critical for credit inclusion” and describing the TransUnion Racial Equity Task Force).

¹¹ For example, FinRegLab’s research has found that bank account cashflow data holds promise for helping borrowers of color who might otherwise face constraints on their ability to access credit. FinRegLab, The Use of Cash-Flow Data in Underwriting Credit: Empirical Research Findings (July 2019), https://finreglab.org/wp-content/uploads/2019/07/FRL_Research-Report_Final.pdf.

¹² See, e.g., Kareem Saleh, There’s A Fix To The Problem Of Biased Algorithms in Lending, Dec. 10, 2019, <https://www.linkedin.com/pulse/theres-fix-problem-biased-algorithms-lending-kareem-saleh/>; Zhang, et al,

be encouraged. At the same time, Congress and other policymakers should adopt measures to reduce the racial disparities in the underlying factors that create the divide in credit scores and other financial data – *i.e.*, reducing the racial wealth gap, combatting housing segregation, preventing employment discrimination, and implementing criminal justice reform.

The experience during the COVID-19 pandemic is instructive. With two stimulus payments and expanded federal unemployment benefits, credit scores stayed stable and even went up for some consumers.¹³ The lesson is simple: if consumers have more financial resources, they can better pay their bills and their scores go up. Racism and its legacy drains precious resources from communities of color, which is directly reflected in credit scores and other financial data.



Mitigating Unwanted Biases with Adversarial Learning, Jan. 2018, <https://arxiv.org/pdf/1801.07593.pdf>.

¹³ Chi Chi Wu, National Consumer Law Center, The Credit Score Pandemic Paradox and Credit Invisibility, Feb. 2021, www.nclc.org/images/pdf/special_projects/covid-19/IB_Pandemic_Paradox_Credit_Invisibility.pdf.