MAXINE WATERS, CA
CHAIRWOMAN

United States House of Representatives
Committee on Financial Services
2129 Rayburn House Office Building
Washington, D.C. 20515

PATRICK MCHENRY, NC
RANKING MEMBER

September 16, 2021

Memorandum

To: Members, Committee on Financial Services
From: FSC Majority Staff
Subject: September 21, 2021, "Preserving the Right of Consumers to Access Personal Financial Data"

The Task Force on Financial Technology will hold a hybrid hearing entitled, "Preserving the Right of Consumers to Access Personal Financial Data" on September 21, 2021 at 10:00 a.m. ET in person in room 2128 of the Rayburn House Office Building, and on the virtual meeting platform Cisco Webex. The single-panel hearing will have the following witnesses.

- **Mr. Tom Carpenter**, Director of Public Affairs, Financial Data Exchange
- **Mr. Raúl Carrillo**, Associate Research Scholar, Yale Law School; Deputy Director, Law and Political Economy Project
- **Ms. Kelly Thompson Cochran**, Deputy Director, FinRegLab
- **Ms. Chi Chi Wu**, Staff Attorney, National Consumer Law Center
- **Mr. Steve Smith**, CEO and co-founder, Finicity

Overview

As financial services companies increasingly employ consumer data to provide new products and services, enormous amounts of data about an individual's personal and financial information are now collected, stored, and at-times made available to third parties. Financial products and services that now rely on consumer-authorized data have the potential to provide improved and innovative new services to consumers, enabling consumers to manage personal finances, automate or set goals for saving, receive personalized product recommendations, apply for loans, and perform other financial tasks.[1] However, debates over how financial institutions should be allowed to use or share consumer data between institutions remain unresolved. The increasing use of consumers' financial data by fintechs and other financial institutions raises policy questions about consumer protections, financial inclusion, privacy, and competition, and how current laws and regulations currently operate in this space.[2]

To better understand the growing use of consumer financial data, the Task Force on Financial Technology held a hearing in November 2019 entitled, "Banking on Your Data: The Role of Big Data in Financial Services."[3] Subsequently, the Consumer Financial Protection Bureau published an advanced notice of proposed rulemaking (ANPR) in November 2020 to solicit information from the public on consumers' right to access their financial information, pursuant to Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (DFA 1033),

---

[1] *See e.g.* MIT Sloan, Fintech, explained (Feb. 4, 2021).
[2] *See* Congressional Research Services, Fintech: Overview of Innovative Financial Technology and Selected Policy Issues (Apr. 28. 2020).
[3] House Financial Services Committee, Banking on Your Data: the Role of Big Data in Financial Services (Nov. 21, 2019).

which provides that financial institutions make available consumer data in their control or possession.[4] Furthermore, in July 2021, President Biden issued an Executive Order encouraging the Consumer Financial Protection Bureau (CFPB) to conduct rulemaking under DFA 1033 to help promote greater competition in the American economy.[5] The purpose of this hearing is to examine recent developments in the data sharing fintech ecosystem.

Consumer Data Market Participants

In recent years, new technologies have led to the development of novel financial service providers that use consumer-authorized data, such as data aggregators and payment processors. Data aggregators help facilitate data sharing between financial institutions possessing consumer data and third parties who seek to provide consumers additional products or services.[6] Consumers may give data aggregators permission to access their information and put into a standardized and summarized format to help make it easier for consumers to manage their money.[7] Payment processors, which help facilitate digital financial transactions between merchants and financial institutions, connect separate financial accounts of a consumer in order to provide services such as peer-to-peer transfers and other payment services.[8] Other users of consumer data include neo-banks (which only have a digital presence and provide apps and other technologies to provide online and mobile banking options),[9] fintechs that partner with a licensed bank to provide a front-end interface, online personal financial management and investment providers, digital savings and budgeting tools, and lenders using consumer financial data for credit decisioning.[10]

Consumer advocates and researchers have argued that consumers, not financial institutions, should have control over how their data is used, but opinions diverge over how consumers should have control of their data.[11] Consumer advocates have also raised questions about consumers' understanding of what they are consenting to, and awareness of which entities are using their data. Data privacy advocates similarly have asked whether notices and solicitation of consent are sufficient, and have raised concerns that consumers may authorize the use of their data for purposes beyond what is understood by the consumer.[12] In response to these concerns, financial institutions and industry groups have launched dashboards and portals that provide consumers insight into which entities hold their data and which would allow consumers to restrict use.[13] Industry and consumer advocates also have expressed a need for regulatory guidance on data use limitations, including possible time restrictions, which the CFPB may consider in its rulemaking.[14]

---

[4] CFPB, Consumer Access to Financial Records, 85 Federal Register 71003 (Nov. 6, 2020).
[5] Executive Office of the President, Executive Order 14036: Promoting Competition in the American Economy, 86 Federal Register 36998 (Jul. 14, 2021).
[6] The CFPB defines data aggregator "as an entity that supports data users and/or data holders in enabling authorized data access." *See* CFPB, Consumer Access to Financial Records, 85 Federal Register 71003 (Nov. 6, 2020).
[7] Examples of data aggregation services include personal financial management services such as Mint and Yodlee. *See* e.g. The Balance, An Overview of Financial Account Aggregation (Aug. 31, 2020).
[8] *See e.g.* Cardknox, The Payments Industry Landscape: What Does It Look Like Today? (last accessed Sep. 8, 2021).
[9] Forbes, What Is A Neobank? (Jun. 24, 2021).
[10] *See* McKinsey & Company, Financial services unchained: The ongoing rise of open financial data (Jul. 11, 2021).
[11] *See e.g.* Adam Levitin, Consumers — not banks — should control access to personal financial data, The Hill (Jul. 6, 2021).
[12] *See* New America, How "Notice and Consent" Fails to Protect Our Privacy, (Mar. 23, 2020).
[13] *See* Deloitte Insights, Building consumer trust Protecting personal data in the consumer product industry (Nov. 14, 2014).
[14] The CFPB's rulemaking on DFA 1033 asks "should . . . restrictions on data access be permitted? For example, should a data holder be permitted to restrict authorized access to consumer data created during, or relating to, certain time periods?" CFPB, Consumer Access to Financial Records, 85 Federal Register 71003 (Nov. 6, 2020).

Regulatory Structure over Consumer Data

In the financial services industry, several federal and state laws cover data privacy. The Gramm-Leach-Bliley Act (GLBA) provides a framework for regulating data privacy and security practices in the financial services industry.[15] GLBA's framework is built upon two pillars: (1) privacy standards that inform consumers about what nonpublic personal information financial institutions can and cannot disclose about them; and (2) security standards that require financial institutions to implement certain practices to safeguard the information from unauthorized access, use, and disclosure. The Fair Credit Reporting Act (FCRA) protects consumer information collected by credit reporting agencies (CRAs) that then use this data to compile credit reports for the purposes of credit decisioning.[16] FCRA imposes certain rules that CRAs must follow in reporting data, such as ensuring accuracy and informing a consumer when an adverse action is taken. Consumer advocates have argued that data aggregators should be considered CRAs and therefore be subject to comply with the FCRA.[17]

The Equal Credit Opportunity Act (ECOA) prohibits discrimination based on gender, race, ethnicity, and other prohibited classes in the extension of credit.[18] As creditors continue to use new technologies to source data used in credit decisioning, questions remain as to how ECOA should apply to ensure data does not perpetuate systemic discrimination in the credit market. Additionally, the Electronic Fund Transfer Act (EFTA) protects consumers engaging in electronic fund transfers.[19] The law is intended to protect a consumer's liability in certain situations, and requires financial institutions and third parties conducting electronic fund transfer services to disclose certain information to consumers.

Screen Scraping, APIs, and Open Banking

Fintech industry technologists have stated that many data aggregators have transitioned from using methods like credential sharing and screen scraping to using a structured data feed or application program interface (API).[20] Screen scraping is a technique for scanning and extracting data from one application by inputting user credentials such as a username or a password and sharing that data with a third party. This can be performed without a direct relationship with the financial firm maintaining the data, raising concerns from advocates and regulators that these methods lack adequate consumer protections and privacy protections, and face cybersecurity weaknesses.[21]

APIs consist of software applications that allow financial institutions to communicate and share consumer data with each other in a secure manner.[22] Using APIs to facilitate data sharing between financial firms may help facilitate open banking, which is the process of enabling data sharing between financial firms and access to financial data or payment systems. Open banking

---

[15] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338, codified in relevant part primarily at 15 U.S.C. §§ 6801-6809, §§ 6821-6827.
[16] Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x.
[17] See e.g. Chi Chi Wu, Data Gatherers Evading the FCRA May Find Themselves Still in Hot Water, NCLC (Jun. 14, 2019).
[18] Equal Credit Opportunity Act, 15 U.S.C. §§ 1691-1691f.
[19] Electronic Fund Transfer Act, 15 U.S.C. §§ 1693-1693r.
[20] *See* Finextra, The new age of Fintech - What you need to know about data aggregators (Feb. 11, 2020).
[21] *See e.g.* Lauren Saunders, Testimony before the U.S. House of Representatives Committee on Financial Services Task Force on Financial Technology regarding "Banking on Your Data: The Role of Big Data in Financial Services," NCLC (Nov. 21, 2019).
[22] IBM, What is an Application Programming Interface (API) (Aug. 19, 2020).

may help facilitate new products and services to consumers, while providing greater financial transparency for consumers on who has access to their data. However, questions exist about how current laws and regulations should apply to the creation of API standards for banks to facilitate data sharing with other financial firms, and how consumer protection, privacy, and cybersecurity concerns are taken into account.

Most APIs depend on bilateral agreements between financial intuitions that hold consumer data (e.g., banks that hold consumers' transaction data), and companies that want to access that data to provide a product or services (e.g., data aggregators or payment processors). These agreements depend on the willingness of the financial institution that holds the data to share access to it, with some traditional financial institution banks being resistant to these partnerships because of perceived security and liability concerns.[23] At the same time, financial institutions that do not have easy access to consumer financial data have expressed that lacking data access impedes their ability to compete with incumbent financial institutions, arguing that because consumers are owners of their data, consumers should have the ultimate authority over which entities can access their data.

DFA 1033 Rulemaking, Executive Order 14036, and Other Recent Developments

In recent years, both industry and consumer advocates have called for regulatory guidance and clarity on consumer data sharing between financial institutions.[24] Section 1033 of the Dodd Frank Act (DFA 1033) provides consumers with a right of access to their financial information, which can include information relating to a transaction, a series of transactions, to an account, and costs, charges, and usage data. However, with the rapidly evolving fintech landscape, the CFPB is currently working on a new regulation to clarify standards around consumer-authorized access to financial data. In November 2020, the CFPB published an advanced notice of proposed rulemaking (ANPR) to solicit information from the public to inform finalization of the rulemaking.[25]

Prior to the publication of the ANPR, the CFPB engaged in stakeholder outreach on this topic. In 2016, the CFPB issued a request for information regarding consumer access to financial records.[26] Using feedback from this request for information, in October 2017, the CFPB outlined nine principles for consumer-authorized financial data sharing and aggregation, that included, among other principles, consumer access and usability, consumer control and informed consent, and data security and accuracy.[27] The CFPB also convened a symposium on the topic in February 2020.[28]

In July 2021, the Biden administration released an executive order on promoting competition in the American economy.[29] The order encouraged the CFPB Director to consider "commencing or continuing a rulemaking under DFA 1033 to facilitate the portability of consumer financial transaction data so consumers can more easily switch financial institutions and use new,

---

[23] *See* Davis Wright Tremaine LLP, Open Banking, APIs, and Liability Issues (Dec. 19, 2019).
[24] *See e.g.* ABA Comments to CFPB Re: ANPR Regarding Consumer Access to Financial Records (Feb. 4, 2021).
[25] CFPB, Consumer Access to Financial Records, 85 Federal Register 71003 (Nov. 6, 2020).
[26] CFPB, Request for Information Regarding Consumer Access to Financial Records, 81 Federal Register 83806 (Nov. 22, 2016).
[27] *See* CFPB, Consumer-authorized financial data sharing and aggregation (Oct. 18, 2017). For a summary of the feedback that informed these principles, *see* CFPB, Consumer-Authorized Financial Data Sharing and Aggregation: Stakeholder Insights That Inform the Consumer Protection Principles (Oct. 18, 2017).
[28] CFPB, Bureau Symposium: Consumer Access to Financial Records, a summary of the proceedings (Jul. 24, 2020).
[29] Executive Office of the President, Executive Order 14036: Promoting Competition in the American Economy, 86 Federal Register 36998 (Jul. 14, 2021).

innovative financial products."[30] As the Executive Order focuses on the enforcement of antitrust laws in many sectors of the economy, consumer advocates have pointed to its inclusion of DFA 1033 to argue that the accumulation of data by large financial institutions and technology companies may be hindering competition in our financial system.[31]

Consumer data breaches such as the September 2017 Equifax data hack, which was settled in January 2020, have also raised concerns over whether fintech companies that use financial data are taking appropriate security measures to ensure consumer data is safe.[32] Consumer advocates have also raised concerns that when consumers provide consent to financial institutions, the burden of liability or risk shifts onto the consumer.[33] Recently, data aggregators and payments processors have been scrutinized for their consumer privacy agreements. For instance, in August 2021, Plaid, a payment processor, settled a $58 million class-action lawsuit over claims that the fintech firm shared unauthorized personal banking data to third party firms without consumer consent.[34]

International Data Sharing Landscape

Several foreign countries have promoted consumer-permissioned data sharing access through APIs, mostly due to cybersecurity concerns.[35] For example, the United Kingdom now requires large banks to adopt open API banking standards with the aim of increasing competition in financial services as a part of its open banking initiative.[36] The European Union's (EU) General Data Protection Regulation (GDPR) establishes a set of rules around personal data throughout the EU.[37] Among other things, it grants individuals data portability with the right to access personal data collected and requires the transmission of one's data to another controller. The EU also adopted the Revised Payment Service Directive (PSD2), which creates API standards for sharing information on payment accounts with third-party payment service providers.[38] In April 2021, the government of Canada released its Finance Ministry's Advisory Committee Report on Open Banking, which set January 2023 as an "ambitious but achievable goal" for launching an open banking system.[39] In August 2021, China enacted its Personal Information Protection Law, a comprehensive privacy law that severely restricts data collection by technology companies. However, many consumer privacy analysts have stated that this law will unlikely limit the country's surveillance apparatus.[40] However, fintech companies have argued that while these regulatory standards are useful, barriers to data sharing may continue to be an issue abroad due to portability difficulties, data sharing fees, and limited data coverage, which can make data sharing difficult in practice.[41]

---

[30] *Id.*
[31] *See* Future of Privacy Forum, What The Biden Executive Order Means For Data Protection (Jul. 16, 2021).
[32] FTC, Equifax Data Breach Settlement (Jan. 2020).
[33] See Center for Financial Services Innovation, Liability, Transparency and Consumer Control in Data Sharing: A Call to Action for Financial Services Providers and Regulators (Sep. 2017).
[34] American Banker, Plaid settles class-action lawsuit for $58 million (Aug. 6, 2021).
[35] *See* U.S. Department of Treasury, A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation, 34 (July 2018).
[36] *Id.*
[37] See Congressional Research Services, EU Data Protection Rules and U.S. Implications (Jul. 17, 2020).
[38] European Central Bank (ECB), The Revised Payment Services Directive (PSD2) and the Transition to Stronger Payments Security (Mar. 2018).
[39] Department of Finance Canada, Final Report Advisory Committee on Open Banking (Apr. 2021).
[40] The Wall Street Journal, China Passes One of the World's Strictest Data-Privacy Laws (Aug. 20, 2021).
[41] John Pitts, Open Banking Must be a Two-Way Street, American Banker (Aug. 4, 2021); *see also* Kat Cloud, PSD2 and GDPR: Are they Enough for Open Finance? Plaid (Sep. 4, 2020).