FinRegLab

900 19th St NW, Studio 6th Fl.
Washington, D.C. 20005
fingreglab.org

BY EMAIL

February 4, 2021

Comment Intake
Section 1033 ANPR
Bureau of Consumer Financial Protection
1700 G Street NW, Washington, DC 20552

RE: Advanced Notice of Proposed Rulemaking on Consumer Access to Financial Records, Docket No. CFPB-2020-0034

FinRegLab is pleased to submit these comments in response to the Bureau's Advanced Notice of Proposed Rulemaking on Consumer Access to Financial Records published on November 6, 2020 (the ANPR). We recognize the breadth of urgent issues facing the Consumer Financial Protection Bureau and the nation at this time, but believe that resolving critical questions about access to financial data would substantially benefit consumers, small businesses, and financial services providers in helping to recover from the Covid-19 pandemic, address longstanding racial wealth gaps, and make U.S. financial systems more generally inclusive, competitive, and responsive to customer needs.

Given that the ANPR is the Bureau's third major initiative to gather feedback on data access issues, we urge the CFPB to move expeditiously on developing concrete rulemaking proposals and working with other policymakers and stakeholders on downstream initiatives.

Background

Established in 2018, FinRegLab is an independent, nonpartisan innovation center that tests and monitors 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.

In early 2020 we published the last in a series of three research reports evaluating the use of cash-flow data in underwriting consumer and small business credit, which we chose as a case study of the potential for customer-permissioned data transfers to spur greater competition

and innovation in financial services markets.[1] FinRegLab Deputy Director Kelly Thompson Cochran spoke about our research findings at the CFPB's February 26 Symposium on Consumer Access to Financial Records.

FinRegLab also published a joint report in fall 2020 with the Financial Health Network, Flourish, and Mitchell Sandler describing federal laws that govern consumer financial data in detail and highlighting various issues that have arisen as data transfers and use have evolved in recent decades.[2] We have also issued a series of research briefs focusing on selected credit access, scoring, and underwriting issues relating to the Covid-19 economic downturn.[3]

These prior reports contain material that is responsive to many of the questions raised in the ANPR. We therefore have not attempted to answer each question separately in this comment letter, but rather are incorporating them by reference and focusing these comments on major themes and recent developments. FinRegLab is not an advocacy organization, but through our research and engagement we work to identify market and policy issues that will be particularly critical in determining the benefits, risks, and scale of adoption for specific data and technology uses.

Discussion

A. Benefits and costs of consumer data access

The generation of consumer financial data has accelerated 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 using information for marketing, verification, and other activities that is generated through consumer interactions with other businesses, such as payroll services companies, merchants, and social media platforms. While traditional credit bureaus and payment networks have transferred consumer data between financial services providers for decades, new types of

[1] See FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: Empirical Research Findings (2019) (summarizing our independent analysis of data from six non-bank financial services providers—Accion, Brigit, Kabbage, LendUp, Oportun, and Petal—conducted in conjunction with Charles River Associates); FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: Small Business Spotlight (2019) (providing a market snapshot of the use of cash-flow data in small business lending markets); FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: Market Context & Policy Analysis (2020) (providing market snapshots of the use of cash-flow data in consumer credit and the underlying system to effectuate data transfers, as well as analyses of policy issues that will shape the realization of potential benefits and risks going forward). These sources are available at https://finreglab.org/cash-flow-data-in-underwriting-credit/.

[2] Financial Health Network, Flourish, FinRegLab & Mitchell Sandler, Consumer Financial Data: Legal & Regulatory Landscape (2020), available at https://finreglab.org/cash-flow-data-in-underwriting-credit/.

[3] FinRegLab, Research Brief, Disaster-Related Credit Reporting Options (2020); FinRegLab, Research Brief, Technology Solutions for PPP and Beyond (2020); FinRegLab, Research Brief, Covid-19 Credit Reporting & Scoring Update (2020); FinRegLab, Research Brief, Data Diversification in Credit Underwriting (2020). These sources are accessible at https://finreglab.org/covid-19/.

intermediaries such as data aggregators have taken on critical roles in financial services markets.[4]

Congress in adopting § 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) has already decided that consumers should have a right to access the data collected and generated by financial services providers for their own benefit. In contrast to past federal consumer financial laws focusing only on selected data about selected financial services, the law applies broadly to information concerning any consumer financial product or service that a consumer has obtained from a covered person, "including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data."[5] Subject to certain exceptions, covered persons must make available upon request whatever such information is within their possession or control in an electronic format that is usable by consumers.[6] And because the Dodd-Frank Act defines "consumer" to include not just individuals but also "agent[s], trustee[s], or representative[s] acting on behalf of … individual[s],"[7] the law is most naturally read to apply not just to requests for data transfers directly by and to individual consumers, but also requests by and to entities that are authorized by consumers to act on their behalf.

This kind of authorized data access substantially increases both the potential benefits and risks of § 1033 relative to direct access alone. Consumers can use directly accessed data to help manage the particular accounts and provider relationships to which it relates and to engage in some secondary activities such as budgeting. But they have limited tools to analyze such data for themselves and are increasingly using data from one financial service provider to obtain financial planning and monitoring services, payment services, and in some cases credit from other financial services providers. Even in the absence of regulations to implement § 1033, 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, with substantial growth in response to the pandemic.[8] The aggregators generally use

[4] Data aggregators generally facilitate customer-authorized data transfers. They developed initially to transfer data collected from bank and other financial institution platforms for use in various personal financial management services, but have expanded to support a variety of other use cases over the last few decades. For a detailed description of the development of the industry, see FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: Market Context & Policy Analysis § 4.2.

[5] 12 U.S.C. § 5533(a).

[6] *Id.* § 5533(a), (b).

[7] *Id.* § 5481(4).

[8] 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. 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 on the overall number of consumers whose data has been subject to authorized transfers are difficult to obtain, in part because surveys ask about use of digital financial services in different ways and a broad range of financial services providers may use authorized data transfers for different purposes. For instance, 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. Nevertheless, growth trends are evident across multiple sources. See, e.g., Alexis Krivkovich et al., How US Customers Attitudes Toward Fintech Are Shifting

consumers' log-in credentials and so-called "screen-scraping" techniques to obtain the data from banking platforms and other provider interfaces, although they are gradually transitioning to methods that provide increased privacy and security protections.[9]

Customer-authorized data flows are thus both fueling consumers' ability to obtain additional financial services from the providers of their choice and providers' ability to deliver immediate services, develop new products, and compete more generally in the marketplace. But the current market is both imposing substantial burdens and risks on consumer and industry participants and is not yet living up to its full potential to drive customer-friendly innovation and competition. As discussed further in the next section, competitive dynamics and coordination challenges between industry actors are complicating authorized data access in the absence of clear regulatory guidance about application of § 1033 and other federal consumer financial laws. Some industry surveys suggest that 40% to 50% of attempts to initiate new data connections may fail due to a variety of technical and market issues.[10] The continuing reliance on log-in credentials and screen-scraping also creates information security, privacy, and accuracy risks for consumers. And the CFPB and other federal regulators have not yet clarified whether and how existing federal consumer financial protections apply to authorized data transfers.

The result is a system where the lack of reliable data access is still substantially complicating financial services providers' ability to develop and deliver more tailored products to customers, while the lack of safeguards is both increasing risk levels and discouraging some consumers from seeking out providers and products that could otherwise offer substantial benefits. 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:

During the Pandemic, McKinsey & Co. (Dec. 17, 2020) (42% of respondents reported having at least one fintech account, with more than 6% becoming a new user during the pandemic); Karl Dahlgren, COVID-19 Pushes Digital Banking Adoption to the Tipping Point, BAI (Sept. 30, 2020) (finding the half of respondents reported increasing use of digital financial services during the pandemic and that 87% intended to continue increased usage going forward); Plaid, The Fintech Effect: Consumer Impact and the Future of Finance (2020) (58% of respondents reported using fintech, with 66% intending to use more often as a result of the pandemic); EY, Global FinTech Adoption Index 2019 at 8 (2019) (reporting 46% fintech adoption rate in the U.S.); The Clearing House, Consumer Survey: Financial Apps and Data Privacy 2 (2019) (54% of banking consumers surveyed reporting using financial apps).

[9] Such methods include using specially generated tokens rather than log-in credentials to authenticate and initiate data access and use of application program interfaces (APIs) for transmission. See FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: Market Context & Policy Analysis § 4.2.

[10] Written Submission of Steven Boms, Executive Director, Financial Data and Technology Association of North America, to the CFPB Symposium on Consumer Access to Financial Records, app. A (Feb. 26, 2020) (reporting connectivity levels in the fourth quarter of 2019 for initial attempts to establish authorized data transfers from various categories of banks and credit unions).

- **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 consumers were rated as "nonprime" even though many of them individually may be likely to repay.[11] These patterns also affect small business credit access, since many lenders consider business owners' personal credit records when making loans. The Covid-19 downturn has created additional uncertainty about the performance of current scoring and underwriting models, as well as concerns that consumers and entrepreneurs who have suffered financial hardships through no fault of their own could face difficulty in accessing credit for years to come based on the way that traditional models treat negative historical information. These concerns are particularly important for African American and Hispanic households and business owners, who are more likely to have limited or negative credit history and high-cost debt than white peers and have been particularly hard hit by the pandemic's health and economic effects.

  FinRegLab's empirical research based on data from six companies using transaction account data and other sources of cash-flow information for underwriting suggests that the data could be valuable in predicting credit risk both among populations that lack traditional credit history and populations who do have credit scores because the data provide somewhat different insights than traditional credit reports.[12] 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, the use of such information in credit underwriting models is relatively limited to date, due in part to challenges in securing reliable data flows and uncertainty about applicable regulatory requirements.[13]

- **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 technology-oriented consumers. Over time, some financial apps that are particularly

[11] FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: Market Context & Policy Analysis § 2.2.
[12] FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: Empirical Research Findings § 5.
[13] As discussed in our research, the use of customer-authorized data transfers for the limited purpose of confirming income or employment is increasing, particularly in mortgage lending due to regulatory verification requirements. However, relatively few companies appear to have developed consumer scoring or underwriting models that incorporate variables derived from transaction account data or other cash-flow sources. Cash-flow analysis has always been a part of small business lending, where adoption of electronic data sources and models appears to be spreading somewhat more rapidly. In both markets, however, reliable data access and regulatory uncertainty have complicated adoption. FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: Small Business Spotlight §§ 4-5; FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: Market Context & Policy Analysis, §§ 4-5. While small businesses' financial data are not covered by § 1033, efforts to facilitate authorized transfers may have positive spillover effects for entrepreneurs particularly to the extent that lenders may consider their personal financial history.

targeted to the needs of low-income households and other underserved populations have been developed by government agencies, nonprofits, and fintech companies; the Covid-19 pandemic has also spurred a range of recent initiatives to help consumers and small businesses cope with the economic downturn.[14] 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 among particular populations.

For example, a recent project focusing on the high levels of high-cost debt among African-American households by Prosperity Now found in a national survey that familiarity with financial advice apps was much lower than with options such as financial coaching and credit counseling, but that participants expressed a tentative openness to such services.[15] Indeed, in a separate group of one-on-one interviews, the number of participants who said that financial apps were or may be appealing was similar to coaching and counseling, particularly in light of the convenience of being able to use at any time and place. However, concerns about information security and challenges in linking accounts were identified as major dislikes and challenges.[16] Prosperity Now later conducted a user-experience study of two apps that most closely corresponded to what interviewees had said they wanted. However, the study found that neither app actually provided the full range of desired services, particularly as to tailored advice on debt repayment issues, and that linking bank and credit accounts was a primary challenge to usage. For instance, many users expressed concerns about 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.[17]

Recent 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 strong interest in both immediate financial management and retirement planning and rapidly increasing levels of digital connectedness more generally.[18]

---

[14] 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).

[15] Prosperity Now, In Search of FinTech for Debt Management and Repayment 25-26 (2020); Prosperity Now, Addressing Debt in Black Communities: A Comprehensive Report Exploring the Potential and Limitations of Services in the Realm of Financial Coaching 5 (2020).

[16] Prosperity Now, Overdue: Addressing Debt in Black Communities 24, 27 (2018).

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

[18] 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.

- **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.[19] In contrast, households of color and low-income consumers are more 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.[20]

Addressing these unmet needs will require more than just solving data ecosystem issues. For example, user-centric design, tailored product features, and application of regulatory safeguards for the specific financial products and services at issue are also important to increasing use and consumer confidence.[21] 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, or where particular customer groups are especially sensitive to concerns about privacy, security, and other aspects of data control.

Customers of smaller financial services providers are another group that may also have a particularly difficult time realizing the potential benefits of authorized data access in the current market because their providers face special challenges in plugging into the broader data ecosystem due to scale and resource constraints. For example, smaller banks and credit unions may be less likely to see authorized data access as a threat to current business lines and may rather view it as a way to retain their current customers and link them to beneficial services

[19] Federal Deposit Insurance Corporation, How American Banks: Household Use of Banking and Financial Services 6-7, 37-38 (2020). Part of the disparity in use of P2P payment services may be due to the fact that such services frequently require links to an underlying bank, prepaid, or credit card account. The percentage of African-American and Hispanic households who lack bank accounts is substantially higher than the percentage of white households (13.8% and 12.2% vs 2.5%, respectively, in 2019), although the percentage of African-American households who use prepaid accounts is substantially higher than Hispanic or white households (14.8% vs. 7.8% and 7.6%, respectively). *Id.* at 2, 6, 33.

[20] *Id.* at 6-7, 37-38. Research suggests that consumers choose such alternative payment sources over traditional services provided via bank accounts because they value certainty about pricing, funds availability, convenience, and other factors. Lisa Servon, The Unbanking of America: How the New Middle Class Survives (2017); Tony Armstrong, The Cost of Being Unbanked: Hundreds of Dollars a Year, Always One Step Behind, NerdWallet (undated).

[21] For a more detailed discussion of the Equal Credit Opportunity Act and other fairness considerations with regard to use of data in credit underwriting and servicing specifically, for example, see FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: Market Context & Policy Analysis §§ 6.1.1, 6.1.2.

that those institutions do not offer. But their ability to provide such access is often limited due to dependence on core processors and other vendors to operate their deposit account platforms, resource challenges, and the fact that their small scale makes negotiation of bilateral contracts with aggregators and other parties difficult. Smaller, newer aggregators and/or financial services providers who want to develop new products and services based on authorized data transfers may also face particular scale and resource constraints. Particularly to the extent that smaller financial services providers may tend to focus on historically underserved populations, this pattern also may affect financial inclusion and the accrual of benefits and risks from authorized data access to different groups of consumers.[22]

B. Competitive incentives and standard setting initiatives

Because the CFPB had not yet clarified whether § 1033 has taken effect and various other questions about legal requirements applicable to authorized data transfers, development of the market to date has been driven in large part by competitive dynamics between different ecosystem participants. These dynamics are shaping both the growing use of bilateral agreements between large individual data holders and intermediaries and efforts to set broader industry standards for data transfer processes. While we see some positive developments in the market, we believe that clear answers to threshold regulatory issues would help to ensure that these industry efforts evolve more quickly in ways that benefit consumers and the market as a whole.

The biggest points of competitive tension concern which parties can access which data for which purposes.[23] As authorized data transfers have grown in volume to support a broadening range of financial services, many data holders have tended to concentrate initially on systems burdens on their platforms and competitive threats from other institutions rather than the potential for their own business lines to benefit from receipt of enhanced information from other sources. Pressure from regulators to manage potential information security and other risks from data transfers have further accelerated the instinct to restrict information flows.[24] We have heard some data holders voice stronger general support in recent months for ensuring better data access to support their own business lines and meet consumer needs and expectations, though such sentiments are not universal and defensive factors may still shape decisions and positions on specific issues. More broadly, implementation and coordination costs remain serious challenges, and pandemic downturn challenges are diverting substantial attention and resources to other issues.

A growing range of industry stakeholders appear to recognize that managing authorized data transfers solely through bilateral agreements and custom-built application program interfaces

[22] Authorized data transfers involving prepaid accounts could also be particularly important to help underserved populations, since such accounts are often used by consumers who are reluctant to use traditional bank accounts due to the risk of overdraft fees and other considerations. FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: Market Context & Policy Analysis at 19; see also n.19.

[23] Liability for unauthorized activity is another substantial source of tension, as discussed further below.

[24] FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: Market Context & Policy Analysis at 50.

(APIs) is suboptimal given the scale and range of data holders, intermediaries, and recipients/users. As a result, participation in the Financial Data Exchange (FDX) and other efforts to build standards and/or infrastructure that can be used on a turnkey basis by a large number of ecosystem participants appear to be attracting growing interest. For example, nearly 200 participants have joined FDX 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 wide range of industry stakeholders, as well as incorporating consumer advocate representation in its working groups. Other group 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.[25]

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, given the wording of § 1033 and the challenges of updating regulations as technologies and market practices evolve.[26] But 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 carefully calibrated balancing between the interests of multiple groups of consumers and financial services providers. Specifically, our interviews with stakeholders suggest that industry coordination incentives would be substantially accelerated and strengthened if the Bureau were to address the following threshold issues regarding the timing, scope, and implication of § 1033 data transfers:

- The deadline for particular groups of covered persons to meet their obligations to make data available upon consumer request under § 1033.

- Guidance on the identities and obligations of agents, trustees, or representatives acting on behalf of an individual consumer for purposes of a § 1033 data request.

- Application of exceptions to § 1033 for particular types of data.

- Whether and how data holders, intermediaries, and recipients are subject to compliance obligations under the Fair Credit Reporting Act (FCRA), the Electronic Fund

[25] FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: 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); Financial Data Exchange, Financial Data Exchange Adds 33 New Members (Jan. 13, 2021); Financial Data Exchange, Financial Data Exchange Releases New Open Finance Standards & FDX API Version 4.5 (Dec. 8, 2020).

[26] The statute directs the Bureau to develop rules that "prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine readable files," yet also directs the Bureau to consult with relevant federal agencies 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 for "financial institutions" under the Gramm-Leach-Bliley Act. 15 U.S.C. § 6801(b).

Transfer Act (EFTA), and the Gramm-Leach-Bliley Act (GLBA) in connection with § 1033 data transfers.

These topics are discussed further below, along with a separate discussion of aspects of these issues that particularly implicate consumer control and privacy. Taken together, we believe that clarity on these issues would substantially strengthen industry incentives to develop technical standards and mechanisms to implement authorized access consistently, efficiently, and safely across the entire market. For instance, small banks may not have the market power to negotiate with their core processors individually to improve the infrastructure and terms of authorized data access, but core processors would be forced to adapt ahead of a regulatory implementation deadline. Settling these issues could also encourage individual data holders to shift their focus from defense to offense by considering more creative ways to use improved data access to benefit their business lines and customers. Clear, consistent regulatory standards for intermediaries—particularly if such companies are supervised regularly by agency examiners—would also increase trust and efficiency among all other ecosystem participants, rather than having to rely solely on individual data holders and recipients to police their counterparties.

With regard to more technical issues such as particular mechanisms for data access and operational reliability standards, the Bureau's most effective role may be to encourage both industry initiatives and sister regulatory agencies to articulate standards rather than to attempt to adopt direct mandates on such topics as tokenization and APIs. While such mechanisms are important to address information security, accuracy, and privacy concerns, as noted above Congress used ambiguous language in § 1033 regarding the Bureau's authority to mandate such mechanisms and chose to leave implementation of general information security standards for financial institutions under the Gramm-Leach-Bliley Act to other agencies. Answering the threshold questions identified above would help both industry and other regulators advance their analyses on associated technical issues to determine if specific regulatory elements or legislative action are needed to further bolster the safety and efficiency of § 1033 transfers.[27]

C. Timing and scope of § 1033 data access

As noted above, settling questions about the timing and scope of § 1033 data access requirements would help to accelerate industry implementation efforts. However, resolving even just this set of questions could be a complex task and requires a strategic approach to ensure that the Bureau can provide necessary clarity in an expeditious manner and sufficient time for complementary initiatives by industry and sister regulators to work through any downstream issues. The following suggestions may be helpful in striking this balance:

[27] To the extent that the Bureau decides that addressing such issues is necessary and appropriate, however, it may be helpful to consider whether authentication/tokenization issues can be separated from building APIs. Eliminating the reliance on credential sharing could significantly reduce information security and liability concerns within the ecosystem even if use of screen scraping techniques for some data collections continues for a longer time period.

- **Determining the deadline for particular groups of covered persons to meet their obligations to make data available upon consumer request under § 1033:** A covered person for purposes of § 1033 is defined generally to include entities that engage in offering or providing any of ten specified categories of "financial products and services" directly to consumers primarily for personal, family, or household purposes, as well as entities that provide specified business-to-business services "in connection with" a direct-to-consumer financial product or service.[28] The Bureau also has authority to define additional activities to be a triggering financial product or service under certain circumstances.[29]

  Because privacy considerations, technologies, implementation burdens, and other factors may vary with regard to particular types of data and financial services providers, it may be advisable to stagger the rulemaking process to prioritize the types of consumer financial products and services that are particularly important to financial health and inclusion, are already the focus of substantial data sharing activities, and/or create substantial questions with regard to overlaps between § 1033 and other consumer financial protection laws. These likely would include (1) extending credit and servicing loans; (2) engaging in deposit-taking activities, money transmission, providing stored value or payment instruments, and providing payments or other financial data processing products or services to consumers; (4) providing financial advisory services to consumers; and (5) processing and maintaining consumer report information or other account information that is used or expected to be used in connection with any decision regarding the offering or provision of a consumer financial product or service.[30] The Bureau could seek comment as it progresses through various stages of the rulemaking process on the similarities and differences in issues for additional categories of covered persons in order to calibrate the list as needed and to begin a second round of rulemaking expeditiously.

  As noted above, clarity regarding implementation timelines would provide greater momentum to industry and sister regulators' initiatives to resolve potential

[28] 12 U.S.C. §§ 5481(5), (6), (15)(A), 5533(a).
[29] *Id.* § 5481(15)(A)(xi).
[30] *Id*. § 5481(15)(A)(i), (iv), (v), (vii), (viii), (ix). Within this list, it would be helpful in particular to consider whether and when payroll processing service providers may be covered persons for purposes of § 1033. There is a debate under state laws as to whether such companies are subject to money transmission licensing requirements, and their information is already being used by some lenders to verify and/or model income. However, this list does not include information about investment products and retirement accounts. Congress may need to act on this issue to ensure consistent data access rights across the entire spectrum of financial products and services that are used by consumers and households. Congressional action would also be needed to give small business owners a right to access financial data relating to their businesses.

downstream issues. The longer the Bureau waits to do its part, the longer any supplemental pieces will also take to put in place.

- **Guidance on the identities and obligations of agents, trustees, or representatives acting on behalf of an individual consumer:** Regulations implementing other federal consumer laws sometimes defer to state law in defining what entities constitute an "agent" of another company for purposes of particular statutory requirements.[31] Under state law, an agent is typically viewed to have a fiduciary duty to subordinate their interests to those of their principal, for instance by exercising appropriate care and diligence, acting within scope of delegated authority, and avoiding self-dealing. Application of these duties under § 1033 to agents of consumers would provide substantive protections, though it might also create some uncertainty as to coverage and potential variation based on geography. Another option would be to issue federal regulations that define the process for authorizing an entity to act as a "representative" of a consumer for purposes of § 1033 and the duties applicable to such entities when "acting on behalf" of an individual consumer under the statute.

- **Application of exceptions to § 1033 for particular types of data:** The statute states that covered persons need not make available confidential commercial information such as scoring algorithms, information collected to detect or prevent unlawful activity, other information that is required to be confidential under law, and information that cannot be retrieved in the normal course of business.[32] But some industry participants have been resisting sharing such items as account routing codes because of concerns that they could be used to perform unauthorized transactions that would incur losses for consumers and/or data holders and pricing information based on an argument that it could be used to reverse-engineer proprietary algorithms despite the fact that the statue specifically mentions data about "costs" and "charges" relating to individual transactions and broader accounts. Clarity on these issues would both help planning on technical transmission issues and resolve competitive tensions.

D. Legal requirements other than section 1033

Uncertainty about the applicability of other federal consumer financial laws to parties who engage in authorized data transfers under § 1033 is also an important issue that both exacerbates potential risks to consumers and complicates interactions between data holders, intermediaries, and recipients/users. Clarifying compliance obligations and taking steps to ensure that all major parties are examined regularly by the CFPB or other regulators as

[31] See, e.g., 12 C.F.R. §§ 1005.3(a) (addressing agents of remittance transfer providers for purposes of the Electronic Fund Transfer Act); 1026 Supp. I, cmt. 2(a)(7)-1 (addressing agents of card issuers for purposes of the Truth in Lending Act).
[32] 12 U.S.C. § 5533(b).

appropriate could substantially increase trust, safety, and efficiency within the broader ecosystem.

Our prior publications catalogue a range of questions on which greater clarity could be helpful.[33] To take just a few examples:

- The Fair Credit Reporting Act creates accuracy, privacy, fairness, and information security protections for "consumer reports" by imposing various obligations on the furnishers of consumer information, the intermediaries who compile the reports, and report users. But federal regulators have not yet clarified whether consumer-authorized data that is transferred via a data aggregator for credit underwriting or other purposes is a "consumer report" or whether and how aggregators and other parties to such transfers are subject to particular FCRA compliance obligations.

- Some aggregators have acknowledged that they meet the definition of a "financial institution" under the Gramm-Leach-Bliley Act, which imposes both privacy and information security obligations on covered institutions. However, updated guidance on how the law's privacy provisions apply to financial institutions that do not have a direct contractual relationship with a consumer and companies that receive consumer information from a financial institution could be helpful.[34] In addition, we understand that some data holders are arguing that GLBA privacy restrictions require them to withhold account routing information and personally identifiable information from authorized transfers, even though GLBA specifically permits information disclosures "with the consent or at the direction of a consumer."[35]

- Clarity as to the application of provisions of the Electronic Fund Transfer Act that limit consumers' liability for unauthorized transactions in cases involving the misuse of consumers' log-in credentials that are shared solely for purposes of retrieving data would help provide certainty to the broader ecosystem to the extent that some authorized transfers continue to rely on this mechanism for data access. Several additional questions are raised about potential liability for unauthorized transactions in the context of payment services providers that use consumer authorized data to facilitate transactions.[36]

---

[33] See Financial Health Network, Flourish, FinRegLab & Mitchell Sandler, Consumer Financial Data: Legal & Regulatory Landscape; FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: Market Context & Policy Analysis §§ 4-6.

[34] As noted above, the Bureau does not have authority to implement the information security requirements. The Federal Trade Commission is engaged in a separate rulemaking to update and clarify expectations for non-bank financial institutions under GLBA. Completion of that rulemaking would also help to reduce risks and facilitate industry interactions in connection with § 1033 transfers.

[35] 15 U.S.C. § 6802(e)(2).

[36] Financial Health Network, Flourish, FinRegLab & Mitchell Sandler, Consumer Financial Data: Legal & Regulatory Landscape at 161-172.

In the absence of clearer regulatory standards and supervision of key market players by the CFPB or other regulators, data holders are using bilateral agreements and other mechanisms to try to limit risk in the broader system, often through use of the processes that they use to manage vendors under third-party service provider requirements.[37] But this is an awkward and inefficient structure. Data holders may be direct competitors of the data recipients and thus may have other incentives to impose restrictions on other ecosystem participants, and intermediaries may not have incentives or leverage to police the conduct of their clients across all potentially relevant issues. Replacing such indirect methods with clear standards and direct supervision by regulators would create greater consistency and confidence in the broader ecosystem for a broad range of stakeholders. Thus, in addition to clarifying substantive standards, exercising the Bureau's supervision authority over market participants is critical, particularly with regard to data aggregators given their key intermediary role.[38]

As discussed further below, the Bureau may find as it works through these issues that existing law either does not extend to or is not a good fit for particular aspects of § 1033 authorized data transfers, and it does not have authority to resolve interpretive questions under GLBA information security requirements as noted above. In such situations, it may be necessary for other regulators or Congress to fill gaps or update the underlying regimes to address important policy concerns. Again, the Bureau's initial analysis will help clarify whether and what downstream issues need to be addressed by other parties to calibrate the risks and benefits of § 1033 data transfers as directed by Congress. This process could begin before the Bureau issues a final rule, for instance when it issues an outline for purposes of conducting the small business review process or a Notice of Proposed Rulemaking that outlines its analysis of authorities and proposed standards.

E. Consumer control and privacy

In both implementing § 1033 and clarifying the application of other federal consumer financial laws, a central question concerns the degree to which consumers will be able to control access and use of their data by aggregators, data users, and other downstream parties. Although we are not aware of substantial issues concerning consumer control and privacy with regard to direct data access by consumers themselves, such issues are critical in the context of data access by authorized entities. The fact that customers must affirmatively authorize access to their information under § 1033 distinguishes such data transfers from various information flows that occur pursuant to provisions of the Fair Credit Reporting Act and Gramm-Leach-Bliley Act,

[37] Financial Health Network, Flourish, FinRegLab & Mitchell Sandler, Consumer Financial Data: Legal & Regulatory Landscape at 107-122; FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: Market Context & Policy Analysis § 4.2.3

[38] The Bureau has authority to examine service providers to various categories of covered persons under 12 U.S.C. §§ 5514(3), 5515, and 5516. In addition, the Bureau can examine non-bank covered persons that are "larger participants" in particular markets for consumer financial products and services after a rulemaking to establish the size thresholds. 12 U.S.C. § 5514(a)(1)(B).

and creates an opportunity not only to access particular financial products and services but to empower consumers to take greater control over their financial lives more generally. Yet given substantial evidence that consumers are already overwhelmed trying to manage data issues in both financial services and other spheres, realizing this potential is extremely challenging.[39]

Our market monitoring and outreach suggest that there currently is substantial variation in consumers' understanding of the actual movement, use, storage, and persistence of data accessed by financial services providers via consumer-authorized processes, and that particular businesses' practices may not always align with consumer expectations or preferences. These variations potentially affect consumers' confidence in the system, the cognitive burdens of managing authorized access, and the degree of risk to consumers from particular transfers.

One part of the problem is that current disclosure practices and consent mechanisms vary by provider and frequently rely primarily on non-standardized terms and conditions documents that consumers likely do not read. Consumers may or may not be aware of the role that data aggregators are playing in obtaining data for use by other financial services providers, and the use of bank logos and other practices have raised concerns about potential consumer confusion as to which parties they are dealing with at particular points in the authorization and transfer process. Some voluntary industry initiatives are working to address these concerns, such as the FDX user experience guidelines for permissioning. Some data holders and aggregators have also begun developing promising monitoring or dashboard tools that make it simpler for consumers to see what types of data are being accessed by which entities and to change access levels going forward, though such tools cannot track data as it is passed further downstream by initial recipients absent substantial contractual coordination or a regulatory mandate to require entities to report back to the initial data source. Accordingly, while these efforts are positive, they are not likely by themselves to produce consistency across the entire market.

Mandating consistent, consumer-friendly disclosure formats and processes pursuant to §§ 1032 and 1033 of the Dodd-Frank Act could help to increase consumer understanding and highlight key areas of difference between individual providers.[40] Yet even if substantially improved, relying solely on notice and consent procedures places a substantial burden on consumers to recognize and evaluate broad variations in market practices and thus risks further increasing information overload dynamics. Defining basic procedures by which consumers authorize or terminate authorization and clarifying minimum data handling standards for entities who are "acting on behalf of" consumers pursuant to § 1033 and other applicable federal consumer financial laws could promote market consistency and help consumers concentrate on the most critical decisions.

In thinking about what activities and issues relating to authorized data access are important to highlight in disclosures and/or regulate substantively, the ANPR's questions probing the differences between data activities relating to the primary purpose for which the consumer

[39] FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: Market Context & Policy Analysis § 6.2.
[40] 12 U.S.C. §§ 5532, 5533.

authorized access and for other purposes are helpful. However, it may also be useful to consider some additional gradations; many of these distinctions appear to be recognized in GLBA privacy provisions although they are not grouped or describe in quite this way:

- Primary use for which consumer has directly authorized access (e.g., evaluation of data in support of an application for credit)

- Supplemental primary uses that are legally required or practically facilitate the financial service provider's ability to deliver the financial product or service that the consumer is seeking (e.g., use of data in servicing/securitizing/selling the resulting loan, auditing and compliance activities, fraud/risk control/information security activities, consumer reporting and risk rating activities, sale of company, etc.)

- Secondary public use (e.g., general law enforcement and legal process, research and product development relating to financial services)

- Secondary commercial use (marketing other products or services by primary or secondary parties, resale for other general commercial purposes)

Focusing on consumer preferences and expectations is important but may not always yield clear lines in determining how to treat various activities. Disclosures can of course shape expectations if they are clear and if the consumer chooses to read them, but consumers often may not. And even if a consumer is not aware of supplemental primary activities such as the use of data in servicing and securitizing a loan or in internal compliance and audit functions, facilitating the provision of the financial product or service that the consumer is seeking is likely consistent with the consumer's overall goals and preferences in interacting with the financial service provider. At the other extreme, secondary commercial uses are more likely to accrue to the benefit of the user company than the consumer and may be more likely to exceed consumer expectations and preferences. To the extent that data is passed to downstream parties with increasingly attenuated incentives to protect the interests of the consumer and/or obligations to help the original recipient company meet its compliance obligations, this also increases risk levels. Indeed, there is a substantial question as to whether a company is "acting on behalf of" a consumer in using data received pursuant to a § 1033 transfer for secondary commercial activities. Requiring particularly clear affirmative consumer consent would provide some safeguards, but still raises broader information overload concerns as discussed above.

Whether and when to consider research and development activities relating to financial services to be a secondary public use or secondary commercial use also raises policy considerations.[41] Such activities can benefit the financial system as a whole by promoting

[41] As an independent, non-profit research organization that designs and executes research to inform market practice and policymaking, FinRegLab's ability to conduct core research activities could be affected by determinations the Bureau makes on this issue during the rulemaking process.

competition, innovation, and fairness, for instance by facilitating the development of new products and services based on more diverse and representative data, as well as by informing improvements in market practices and regulation.[42] Research and development uses may be consistent with consumer expectations in other spheres, for instance in the use of data regarding consumers' use of particular websites to improve functionality over time, although such expectations may not extend to use by other companies or to improve other product offerings. And the specific downstream benefits to the individual consumer may depend on his or her subsequent demand for such financial services over time.

Current regulatory regimes under FCRA and GLBA manage this tension by providing more flexibility with regard to the use and disclosure of data without personally identifiable information, although neither set of regulations currently provides detailed criteria for what information is sufficiently anonymized to trigger the more flexible treatment. Greater clarity on this issue would be helpful in light of both recent research highlighting limitations and risks with regard to de-identification and the emergence of new "privacy enhancing technologies" that work to minimize the possession and transfer of personal data while facilitating beneficial use cases. More broadly, however, there may also be a need to consider differences between § 1033 and the other regimes in light of the former's focus on access by consumers and entities authorized to act on their behalf. This may be an area where further action by both the CFPB and Congress could help to more fully effectuate § 1033's potential effects on innovation and competition by providing particular structures to help facilitate the development of products and services that will help consumers derive further benefits from their data.

F. Data security, accuracy, and other topics/information

Data security and accuracy are important issues for all stakeholders in the ecosystem for consumer permissioned transfers, and liability in connection with data breaches and unauthorized transactions is a critical issue particularly to the extent that most transfers are still being effectuated via sharing of log-in credentials. Existing regulatory regimes such as the Gramm-Leach-Bliley Act, Fair Credit Reporting Act, and Electronic Fund Transfer Act provide potential tools for managing such concerns, but they were not specifically designed for the new ecosystem that is emerging around authorized data transfers and may not always provide optimal mechanisms for managing particular issues. This is one of the reasons that positioning the Bureau to increase coordination with other agencies and Congress about potential downstream issues is so important.

As discussed above and in our previous reports, GLBA provides a framework for information security requirements for all "financial institutions," a term that includes depository institutions, lenders, financial advisors, and a range of data intermediaries. However, the Bureau has authority only with regard to GLBA privacy provisions, not its information security

[42] In this respect, to ANPR question 12, consumers' individual decisions about whether to authorize data access can entail significant negative or positive externalities on other consumers, data holders, intermediaries, and recipients by providing access to data that can be used to improve product offerings over time.

requirements. Coordination with other federal agencies will thus be critical to clarify and confirm both sets of compliance obligations for all parties in the ecosystem. In particular, the Federal Trade Commission's current rulemaking to update information security requirements will be a critical component to ensure that data intermediaries—including both traditional consumer reporting agencies and data aggregators—are subject to strong, consistent, modern standards. Relying solely on private incentives and indirect policing through third party service provider guidance is not sufficient for the reasons discussed above. Further, supervision gaps are an important issue for key non-bank intermediaries, since the Bureau does not have authority to examine for GLBA information security compliance and the FTC does not have authority to conduct examinations more generally. Accordingly, Congressional review of this issue is warranted.

Inaccurate data is a potentially serious concern because it undermines the quality and value of any financial services provided based on such data. While accuracy in credit scoring and underwriting is a longstanding policy concern that prompted enactment of the Fair Credit Reporting Act, accuracy issues could also have potential effects on the quality of personal financial management and payments services. The most obvious accuracy concerns with regard to authorized data transfers are the use of screen scraping rather than APIs and whether aggregators are required by federal law to correct any errors that they may have introduced into consumer data. However, there may also be deeper questions with regard to the accuracy of information relating to transaction accounts and other financial products as it sits initially with data holders. The Electronic Fund Transfer Act provides some mechanisms for error correction, though it is primarily focused on addressing account administration and liability for unauthorized transactions rather than the accuracy of the data for use in secondary activities that may occur years later. It would be helpful for the Bureau to gather additional information on these issues to access the need to manage accuracy risks more broadly, and whether existing requirements under EFTA or the FCRA can be appropriately calibrated to the emerging ecosystem.[43]

Finally, liability with regard to data breaches and unauthorized transactions that involve multiple parties is a complicated topic even outside of the new data ecosystem for authorized transfers. For example, while payment systems have evolved to handle the resolution of individual unauthorized transactions, they have struggled to sort out liability in large-scale privacy breaches of major retailers. Concerns about data breaches at large aggregators and data users raise similar scale issues, particularly if they involve log-in credentials as well as other types of data, but the market mechanisms are less evolved and application of existing regulatory protections are unclear. Addressing basic questions under the Electronic Fund Transfer Act such as how unauthorized transaction provisions apply to the misuse of log-in

[43] FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: Market Context & Policy Analysis § 6.1.1.2.

credentials by particular parties would be an important first step in providing clarity.[44] However, this may also be an area in which Congressional action is needed, for instance to provide greater accountability for data handling as information passes to downstream parties.[45]

Conclusion

The use of authorized data transfers has been growing for more than two decades, and § 1033 itself is now more than 10 years old. Particularly given the need for potential downstream work by industry, fellow regulators, and/or Congress, further delays in clarifying threshold questions under § 1033 and other federal consumer financial laws would increase the risk of bad outcomes and/or expensive transitions. Complementary efforts by other actors need not wait until a Bureau rule is finalized, but a clear roadmap of the Bureau's authorities, interpretations, and substantive proposals will help to sharpen the other initiatives' focus and urgency. We urge the Bureau to act expeditiously to ensure that § 1033 is implemented safely, efficiently, and consistently across financial services markets.

Thank you again for the opportunity to comment on these issues.

Melissa Koide

Melissa Koide
CEO and Director

Kelly Thompson Cochran

Kelly Thompson Cochran
Deputy Director

[44] The Bureau also has authority to adopt bonding or other financial requirements to ensure that non-bank financial services providers that are subject to its supervision jurisdiction are able to meet their obligations to consumers. 12 U.S.C. § 5514(a), (b)(7).

[45] For a more detailed discussion of these and other potential Congressional actions to help strengthen the emerging ecosystem, see FinRegLab, The Use of Cash-Flow Data in Credit Underwriting: Market Context & Policy Analysis § 7.3.