February 4, 2021

Dave Uejio
Acting Director
Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552

**Re: Advanced Notice of Proposed Rulemaking Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act, Docket No. CFPB-2020-0034 or RIN 3170-AA78**

Dear Acting Director Uejio:

Consumer Reports writes today in response to the Advanced Notice of Proposed Rulemaking Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act, Docket No. CFPB-2020-0034 or RIN 3170-AA78. Consumer Reports is an expert, independent, non-profit organization whose mission is to work for a fair, just, and safe marketplace with and for all consumers and to empower consumers to protect themselves.[1]

Section 1033 of the Dodd-Frank Act provides for consumer rights to access the financial information companies collect and hold about them. Consumers may seek access to their data from service providers for a variety of purposes, including to put this information to use in other services. For example, a person may want to have a budgeting app access their credit card purchases, payments and other account information and combine it with other financial information in order to get a more complete picture of their household finances. While data access can have real benefits for consumers, it can also pose risks if done without adequate safeguards to ensure consumer data privacy and security, secure consumer consent, and ensure rights to review and correct information companies have about them.

[1] CR works for pro-consumer policies in the areas of financial services and marketplace practices, antitrust and competition policy, privacy and data security, food and product safety, telecommunications and technology, travel, and other consumer issues in Washington, DC, in the states, and in the marketplace. Consumer Reports is the world's largest independent product-testing organization, using its dozens of labs, auto test center, and survey research department to rate thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

Herein, CR comments on the benefits and risks of the consumer financial data ecosystem, as well as the other topics of the ANPR: competitive incentives; standard-setting; access scope; consumer control and privacy; and data security and accuracy. In these comments, we urge the Bureau:

- To move forward with a rulemaking for Section 1033 to ensure consumers' fundamental privacy rights;
- To curb providers' practices that imperil consumer privacy and security, and mandate data minimization;
- To ensure meaningful consumer consent to any collection, processing and sharing of their data by any entity in the chain and prohibit some secondary uses of that data;
- To provide consumers a clear right to review and correct information companies have about them, and to have a broad deletion right in accord with existing rules; and
- To use its UDAAP authority to crack down on unsubstantiated claims about the use of artificial intelligence and machine learning in financial services, and take the steps necessary to ensure algorithmic accountability.

**Background**

The driver behind the need for data access rules is the rise of digital financial services, colloquially known as "fintech." The rise of the digital financial ecosystem is changing how consumers bank, borrow, and pay. However, while they are often seen as fully new, a scan of the products touted as "fintech" quickly reveals that few, if any of these products are truly novel. Most "fintech" offerings fall within established legal definitions of products and services for deposit-taking, payments and money transmission or lending. A few examples: point of service loans have existed for decades, but they used to be called "lay-away." Several forms of early wage access are payday loans in fintech garb.[2] Person-to-person payments are an extension of the text message P2P functionality many prepaid cards had before 2010. Many of the automated savings programs mimic the essentials of Christmas Club accounts that have been around for decades. The rules for banking and payments are well-established and, while now contested, should apply to newer stylings of these products and services.

While product verticals remain steady in financial services, 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. For example, a department store's layaway counter would hold only the barest contact information for a purchaser while today's point of service lenders can, depending on their terms of service, collect vast quantities of financial and non-financial information about their users. Similarly, while a traditional credit card payment implicates a merchant, two banks and a payments processor,[3] a payment made with a

[2] Sidney Fussell, The New Payday Lender Looks a Lot Like the Old Payday Lender, https://www.theatlantic.com/technology/archive/2019/12/online-banking-lending-earnin-tip/603304/.
[3] Susan Herbst-Murphy, Clearing and Settlement of Interbank Card Transactions: A MasterCard Tutorial for Federal Reserve Payments Analysts, at 22,

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, with its partners, consumer data.

While some data collection is necessary and appropriate, CR research has documented that often digital financial data collection far exceeds this baseline.[4] Service providers justify all-encompassing surveillance of users in the name of "analytics" or "product improvement." In many instances, financial service providers also reserve broad rights to use consumer data for unrelated purposes, including targeted advertising, and to share user data widely.[5] The roles of some of the parties involved are not always clear to consumers. For example, there are several lawsuits pending that hinge on how the role of data aggregators is (or was) disclosed to consumers,[6] and whether or not consumers have consented to the sale of their data.[7]

In 2017, the Bureau published its Consumer Protection Principles: Consumer–Authorized Financial Data Sharing and Aggregation.[8] These principles contain best practices, but best practices alone, as the above examples illustrate, have not created "a robust, safe, and workable data aggregation market that gives consumers protection, usefulness, and value."[9] Consumers need strong protection under law. Specifically, there is an urgent need for a comprehensive legal framework for consumer data access, one that clearly protects consumers' fundamental privacy right, establishes consumer rights and remedies in the event of unauthorized access, inaccurate information, or other fraud or error as a result of data sharing.

We urge the Bureau to approach any rulemaking for consumer access to financial records with a skeptical view not only of potential promises of technology and innovation. There is a

---

https://www.philadelphiafed.org/-/media/consumer-finance-institute/payment-cards-center/publications/discussion-papers/2013/D-2013-October-Clearing-Settlement.pdf.

[4] See eg . https://files.consumerfinance.gov/f/documents/cfpb_tetreault-statement_symposium-consumer-access-financial-records.pdf and https://www.consumerreports.org/digital-payments/mobile-p2p-payment-services-review/

[5] See for example this from the Plaid End User Privacy Policy: "We may collect, use, and share End User Information in an aggregated, de-identified, or anonymized manner (that does not identify you personally) for any purpose permitted under applicable law." https://plaid.com/legal/ios/#how-we-use-your-information.

[6] https://www.plaidprivacylitigation.com/ and https://stories.td.com/us/en/article/td-bank-files-trademark-counterfeiting-and-infringement-lawsuit-against-plaid-in-the-u-s?

[7] Letter here: https://www.wyden.senate.gov/imo/media/doc/011720%20Wyden%20Brown%20Eshoo%20Envestnet%20Yodlee%20Letter%20to%20FTC.pdf; press coverage here: https://www.wsj.com/articles/lawmakers-call-for-investigation-of-fintech-firm-yodlees-data-selling-11579269600

[8] *Consumer Protection Principles*, Consumer Fin. Protection Bureau (Oct. 18, 2017), *available at* https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

[9] *Id.* at 1.

common refrain that any approach must be technology neutral.[10] While we understand the desire to have regulations that do not change as quickly as technology, we urge the Bureau to remember that even if regulation is technology-neutral, technology itself is not. Technology is often first directed at and used against the interests of people of color and people with lower wealth.

Some newer financial products and services may pose direct risks to consumers with the least power to avoid them. We therefore urge the Bureau to make a critical assessment of newer technologies, and in particular those that Hoover up massive amounts of consumer data, to ensure that already underserved and/or badly served communities do not worsen harms these communities are already subject to, including racialized surveillance. The reasons consumers are functioning outside the financial mainstream in the United States are largely structural.[11] Digital apps, and particularly the surveillance inherent in many, are not a fix for structural problems. We urge that the recent Bureau approach to innovation, with its loosening of rules and lax oversight, be jettisoned in favor of ensuring consumer privacy, preventing algorithmic bias, and upholding basic consumer protections by established product type.

It is time for rules for consumer financial data access, specifically rules that demarcate appropriate boundaries for the collection, processing, holding and "sharing" of consumer financial data, and rights of consumers to review and correct this information, and to ask companies to delete information. Submitted below are CR's recommendations for how the promise of digital financial services can be achieved while ensuring consumers' fundamental privacy rights.

**A. Benefits and costs of consumer data access**

Digital innovation brings benefits to consumers. Digital financial services offer rapid speed and great convenience. For example, it's far more convenient to pay a buddy back with a few taps on a phone than to run to an ATM to get cash. Digital financial services add new services often, tailoring services to consumer needs and desires. A recent example is the person-to-person payment service Venmo which began with just that one payments feature, adding mobile remote deposit capture, branded as "check cashing" to its app.[12] (This is a feature banks have offered customers for more than a decade.[13])

---

[10] See for example, at 177, https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf

[11] Unbanked Americans, when asked cite the costs associated with banking, and - first and foremost - not having enough money to keep in account as the main reasons for not having a bank account. https://www.fdic.gov/householdsurvey/2017/2017execsumm.pdf at 4.

[12] "Cash your stimulus check without a trip to the bank," https://venmo.com/about/stimulus/?gclid=CjwKCAiA9bmABhBbEiwASb35V8v394ArKwOmzqCrVvI7T_wN6-zTwAN_qch3KFcapSUqnNxqY3FEbRoCe-QQAvD_BwE&gclsrc=aw.ds

[13] https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum09/primer.html

Any number of products and services are built around consumer permissioned data, including tax preparation, budgeting,[14] automated savings,[15] "overdraft avoidance,"[16] bill negotiation,[17] underwriting,[18] and wealth management,[19] to name just a handful. Millions of consumers rely on these services, and while the benefits of each vary in the particulars, few would wish completely to forsake the conveniences of digital-first financial services.

Consumers face several risks, however, in permissioning data. Long-standing problems with particular products and services do not cease to exist when these services are digitized. For example, credit reports are riddled with errors,[20] and while, for example, digital services such as Credit Karma offer tools that help users dispute errors,[21] consumer complaints about credit report errors remain high.[22] The many companies involved in these services - the consumer-facing service provider, the data aggregator facilitating access, and the source of the data the consumer permissions, for example - may not all be known to the user, and the company that they perceive to be the one they are interacting with may not be the one legally responsible or willing to fix a problem should one arise.

In some cases, the ways in which consumer data is permissioned might itself lead to errors or pose a security risk. All manner of digital financial services rely on screen-scraping, including budgeting, savings and credit-building services. Screen-scraping is widely recognized as a less secure and less accurate method of permissioning information sharing than other methods,[23] and there is not a clear legal framework that accounts for risks associated with screen-scraping.[24] Several years ago, banks tried to make consumers liable for fraud on their accounts if they

---

[14] https://mint.intuit.com/
[15] https://digit.co/
[16] https://plaid.com/customer-stories/qapital/
[17] https://www.truebill.com/
[18] See eg Experian Boost, in which consumers permission additional data in the hope of raising their credit score: https://www.experian.com/consumer-products/score-boost.html. The linking of accounts for Boost is done via data aggregator Finicity: https://www.experian.com/consumer-information/account-aggregation-solutions.
[19] https://resources.yodlee.com/wealth-management/envestnet-yodlee-financial-wellness-solution
[20] https://www.ftc.gov/news-events/press-releases/2013/02/ftc-study-five-percent-consumers-had-errors-their-credit-reports
[21] Some services do facilitate credit report disputes, either for free or for a fee. See eg Credit Karma: https://www.creditkarma.com/advice/i/credit-karma-direct-dispute#A and Credit Sesame: https://help.creditsesame.com/hc/en-us/articles/360003458272-There-is-something-incorrect-on-my-credit-profile-.
[22] https://uspirg.org/reports/usp/analysis-cfpb-complaints-surge-during-pandemic-led-credit-report-complaints
[23] https://www.consumerreports.org/privacy/consumers-get-more-control-over-banking-data-shared-with-financial-apps/
[24] Consumer Financial Protection Bureau, Consumer-authorized financial data sharing and aggregation Stakeholder insights that inform the Consumer Protection Principles, Ability to dispute and resolve unauthorized access, 10:

shared their account credentials.[25] CR found several digital financial services that put users on the hook for any losses associated with "use of or access to" their services.[26] Consumers thus had no clear legal right to resolve issues that stemmed from the risks intrinsic to these products. Given that all the parties involved in the digital financial ecosystem are rich targets for hackers,[27] it seems only a matter of when, not a matter of if, these policies will be tested. As noted in more detail below, consumers need protection from harms they cannot reasonably avoid, and a right to remedy errors that occur.

Even though their own practices or those of the services they rely on to function may introduce errors, few digital finance companies offer consumers a clear path to review or correct data held by the provider. In some instances, that is appropriate. For example, although credit report data may be accessible through an app, consumers still must follow the rules of the Fair Credit Reporting Act to dispute errors. However, several apps that CR evaluated that offer access to consumer credit reports also have privacy policies that enable these services to collect and keep far more information about users than what is contained within their credit reports, but offer limited if any consumer rights to review and correct that data. For example, Credit Karma allows users to edit "name, home address, gender, marital status and annual household income."[28] Meanwhile, Credit Karma collects information when users give it to them, from "automatic technologies and when we ask others for it,"[29] which likely includes far more than name, address, marital status and household income. Additionally, not enough companies make clear to users if or how they can have their personal information deleted from service provider files

---

https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf.

[25] https://www.reuters.com/article/us-column-weston-banks/why-banks-want-you-to-drop-mint-other-aggregators-idUSKCN0SY2GC20151109

[26] All the service providers have general indemnity provisions that would seemingly insulate them from liability should a consumer's bank account be breached as a result of using these services. Albert: "You will indemnify and hold harmless Albert and its officers, directors, employee and agents, from and against any claims, disputes, demands, liabilities, damages, losses, and costs and expenses, including, without limitation, reasonable legal and accounting fees arising out of or in any way connected with (i) your access to or use of the Services…" Albert also limits anything it will pay for consumer losses to $100. https://albert.com/terms/. Truebill: "YOU ACKNOWLEDGE AND AGREE THAT WHEN TRUEBILL IS ACCESSING AND RETRIEVING ACCOUNT INFORMATION FROM THIRD PARTY SITES, TRUEBILL IS ACTING AS YOUR AGENT, AND NOT AS THE AGENT OF OR ON BEHALF OF THE THIRD PARTY THAT OPERATES THE THIRD PARTY SITE." https://www.truebill.com/terms#account-information-from-third-party-sites; Trim: "You agree to indemnify and hold Trim, its affiliates, officers, agents, employees, and partners harmless from and against any and all claims, liabilities, damages (actual and consequential), losses and expenses (including attorneys' fees) arising from or in any way related to any third party claims relating to (a) your use of the Services (including any actions taken by a third party using your account)..." https://www.asktrim.com/tos

[27] https://krebsonsecurity.com/2019/08/the-risk-of-weak-online-banking-passwords/#more-48391

[28] https://support.creditkarma.com/s/article/How-do-I-change-my-personal-information-US?topParent=Manage_Your_Account_US&parentCategory=Manage_Your_Account_US&selectedCateg=Manage_Your_Account_US&parentCategoryLabel=Manage+Your+Account&currentCategLabel=Manage+Your+Account.

[29] https://www.creditkarma.com/about/privacy-20200101

should they leave the service. Credit Karma, for example, keeps user data for two years after users cancel before "anonymizing" it, and then perhaps keeps it forever, as their privacy policy does not say if anonymized data is ever deleted.[30]

As discussed in more detail below, another risk of data permissioning is service providers' lack of transparency about their data collection, use, and sharing practices, as is the expansive, excessive data collection done by far too many actors in the financial data ecosystem, whether the practice is transparently disclosed or not. Surveillance itself is a privacy harm, and consumers have a privacy interest in controlling commercial collection of their personal information.[31]

**B. Competitive incentives and authorized data access**

Consumers may experience difficulties in moving their business from one service provider to another. For example, CR has documented how it can be a hassle to move one's money from one financial institution to another.[32] We think that a clear data access right, with appropriate safeguards, will ensure that consumers have the right to safely, quickly and easily port their information, including account details such as account numbers and interest rates, among service providers. This right will ensure robust competition and prevent consumers from being "trapped" at a particular financial service provider.

**C. Standard-setting**

Various businesses are working on standards for consumer data security and privacy. CR, along with others, has developed an open-source digital privacy and security standard, the Digital Standard which works across industries and product types. Specific to financial services, CR is engaged in standard-setting efforts. CR is a member of the Financial Data Exchange (FDX).[33] FDX "is dedicated to unifying the financial industry around a common, interoperable and royalty-free standard for the secure access of user permissioned financial data," and "exists chiefly to promote, enhance and seek broad adoption of the FDX API technical standard and is dedicated to five core principles of user permissioned data sharing: Control, Access, Transparency, Traceability and Security."

---

[30] https://www.creditkarma.com/about/privacy-20200101

[31] Justin Brookman & G.S. Hans, *Why Collection Matters: Surveillance as a De Facto Privacy Harm*, Future of Privacy Forum Big Data & Privacy Workshop Paper Collection (2013), https://fpf.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.

[32] For more on ensuring consumer choice in banking, *see Trapped at the Bank: Removing Obstacles to Consumer Choice in Banking*, Consumer Reports (May 20, 2012), https://advocacy.consumerreports.org/research/trapped-at-the-bank-removing-obstacles-to-consumer-choice-in-banking/.

[33] "FDX is setting the standard for secure financial data sharing." https://financialdataexchange.org/

While we are eager to see the FDX API technical standard gain broad acceptance, more needs to be done. However laudable voluntary efforts are, they are inherently limited. Consumers need protections in law so that bad actors can be stopped.

**D. Access scope**

The Dodd-Frank Act defines "consumer" as "an individual or an agent, trustee, or representative acting on behalf of an individual." Consumers have very little idea about what data is collected and shared when they use financial apps.[34] Financial apps may not make clear the role of data aggregators in facilitating data sharing, and consumer consent to the data aggregator's practices may be secured by consumers clicking "agree" to the provider's terms without being prompted to consider - or consent to - the role of the data aggregator.[35] Therefore consumers may not know when they have authorized an agent, and may not know much if anything about the agent's practices. We urge the Bureau to issue rules that mandate that every entity secure direct, individual, meaningful consent before being considered "an agent, trustee, or representative" of an individual consumer for purposes of implementing section 1033 access rights. CR found that in some instances, consumer consent to data aggregators' practices is secured by having consumers click "agree" to first order agreements that bind them to data aggregators privacy policies and terms of service.[36] Agents "acting on behalf of an individual" should not include data aggregators if consumer consent is buried two or more clicks down.

There must be clear disclosure of the role or roles of third parties in facilitating data access, a method of ensuring meaningful consent, and such permission should only be for a limited scope - to carry out the purposes for which the consumer has sought the service - and for a limited duration. Moreover, consent must only be valid for limited data collection, again only what is necessary for the service, and consumers should have the right to revoke access at any time. Further,consumers should have, in accordance with existing laws and regulations, the right to have their information deleted from provider files.

In addition to establishing a requirement that every entity in the chain secure from consumers clear consent for limited data collection for a particular purpose and for a particular duration, consumers need the Bureau to clarify their rights under the Electronic Funds Transfer Act (EFTA) as implemented by Regulation E (Reg E). Two areas need particular attention. The Bureau should make clear that consumers retain their Reg E error resolution rights when they

---

[34] The Clearinghouse has done extensive consumer research that raises questions about what consumers understand about the ways in which service providers collect and share their data. See for example, Consumer Survey, Financial Apps and Consumer Privacy, https://www.theclearinghouse.org/connected-banking/consumer-research.

[35] https://files.consumerfinance.gov/f/documents/cfpb_tetreault-statement_symposium-consumer-access-financial-records.pdf

[36] https://files.consumerfinance.gov/f/documents/cfpb_tetreault-statement_symposium-consumer-access-financial-records.pdf

permission data access, and that any waiver of those rights is against public policy. Second, the Bureau should make clear that in some circumstances, data aggregators are "financial institutions" for the purposes of Reg E. Reg E includes an expansive definition of financial institution, and such institutions are covered if they directly or indirectly hold an account belonging to a consumer, or issue an access device and agree to provide a consumer with certain electronic fund transfer services.[37] We have seen instances where digital savings apps secure a users' written authorization for preauthorized transfers, including preauthorized transfers in varying amounts, and yet appear to disclaim or do not make clear that consumers using these services have Reg E error resolution rights.[38] While we believe that Regulation E is clear on this point already and that no regulatory changes are needed, we are calling on the Bureau to remove any uncertainty.[39]

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. There remains a lack of certainty as to what kinds of information are subject to the Section 1033 access requirements.[40] We urge the Bureau to consider that some data is simply too sensitive for collection and sharing, and should simply be out of bounds. This includes medical information. We further urge that the Bureau take a hard look at the ways in which service providers may be collecting and sharing data culled from social media, and consider restricting its collection, imposing strict limits on sharing, and banning the sale of it for any purpose.

**E. Consumer control and privacy**

Consumers worry about privacy and security.[41] They also perceive that there is very little they can do to exercise their privacy rights, as validated by a recent participatory research study by

---

[37] Section 1005.10

[38] https://advocacy.consumerreports.org/wp-content/uploads/2020/03/Final-Savings-Letter-March-9-2020.pdf

[39] Consumer Reports comment on the Consumer Financial Protection Bureau's Inherited Regulations and Inherited Rulemaking Authorities, https://www.regulations.gov/document?D=CFPB-2018-0012-0039.

[40] https://finreglab.org/wp-content/uploads/2020/10/Financial-Data-White-Paper.pdf at 32

[41] In a CR nationally representative survey, 65 percent of Americans said they are either slightly or not at all confident that their personal data is private and not distributed without their knowledge, https://www.consumerreports.org/digital-security/online-security-and-privacy-guide/. In 2020, CR research found that 85% of Americans are either very concerned or somewhat concerned about the amount of data online platforms store about them, and 81% of Americans are either very concerned or somewhat concerned that platforms are collecting and holding this data about consumers in order to build out more comprehensive consumer profiles; https://advocacy.consumerreports.org/press_release/consumer-reports-survey-finds-that-most-americans-support-government-regulation-of-online-platforms/.

CR.[42] The current state of things is a confusing mess, and puts far too much responsibility on consumers to secure their own privacy.

Provider privacy policies across industries lack transparency.[43] Current law mostly allows companies to describe their data practices however they want and generally holds companies responsible only if they actively lie to consumers about what they do. CR's 2018 review of P2P providers' privacy practices revealed providers were often vague in their descriptions of data collection,[44] and their agreements reserved broad rights to collect and share data for unrelated purposes, including targeted advertising.[45] Similarly, the disclosures required by the Gramm-Leach-Bliley Act, 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,[46] are so confusing that consumers are unlikely to exercise their rights.[47]

Even if privacy policies were perfectly clear about provider practices, consumers would probably remain in the dark about what information is collected and shared because consumers do not read the terms of service or privacy policies.[48] This problem is exacerbated by the multiple layers of agreements most financial services applications require consumers to consent to in order to use them. Depending on the service and its features, users may be bound to two or three, or a dozen or several dozen agreements. For example, the investing service Robinhood lists 37 different agreements in its Disclosure Library.[49] It is simply not efficient or practicable for consumers to read disclosures; a study by Aleecia McDonald and Lorrie Cranor estimated that

---

[42] Consumer Reports worked with Californians attempting to exercise their rights under the California Consumer Privacy Act. Many reported great difficulty in locating the means for exercising the right to prevent the sale of their data, and found in particular that data brokers' opt-out processes to be particularly onerous. https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf

[43] Marcus Moretti & Michael Naughton, *Why Privacy Policies Are So Inscrutable*, The Atlantic (Sept. 5, 2014), https://www.theatlantic.com/technology/archive/2014/09/why-privacy-policies-are-so-inscrutable/379615/.

[44] Why Apple Pay Is the Highest-Rated Mobile P2P Payment Service, https://www.consumerreports.org/digital-payments/mobile-p2p-payment-services-review/.

[45] Peer-to-Peer Payments Are Generally Safe, But Consumers Must Be Aware of Risks https://www.consumerreports.org/digital-payments/peer-to-peer-payments-are-generally-safe-but-consumers-must-be-aware-of-risks/

[46] 15 U.S.C § 6802(b).

[47] *Statement of Travis Plunkett, Legislative Director, Consumer Federation of America on Behalf of the 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.

[48] Caroline Cakebread, *You're not alone, no one reads terms of service agreements*, Bus. Insider (Nov. 15, 2017), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11.

[49] https://robinhood.com/us/en/about/legal/

reading every site's privacy policy would take users over 244 hours per year, at a collective societal cost in wasted opportunity of over $600 billion.[50]

Given that consumers rarely read first order agreements, it is unlikely they are reading the agreements most relevant here: those of the data aggregators on whom many financial apps rely. Consumers may find deep in the terms or service or privacy policies that agreeing to use a service binds them to the terms of a data aggregator. If consumers did read the privacy policies of data aggregators, they might be surprised at how much information was collected about them, how widely it is shared, and how long it is held. For example, data aggregator Plaid's agreement not only allows Plaid to collect information about users from the accounts users link, but also "from other sources."[51] While Plaid's terms state that while user data is not sold, it is shared.[52] Plaid claims user information is not shared without the user's "consent."[53] This seems to stretch the meaning of the word consent. Is consent meaningful if it is the result of a click on a first order agreement that binds the user to Plaid's terms, as is the case with some financial apps?[54] The Bureau must mandate clear consent to data collection by every service provider in the chain.

The burden cannot fall to consumers alone. The Bureau should also take additional steps. Given the documented overcollection of consumer information, we urge the Bureau to mandate that providers practice data minimization, collecting no more than is necessary for the provision of their services and to comply with the law. There also must be rules requiring deletion of consumer data, as CR research has shown that providers sometimes hold user information indefinitely,[55] making them a rich target for hackers. Some primary data collection and use, and some secondary sharing should simply be out-of-bounds because of the sensitivity of the data

---

[50] Aleecia M. McDonald and Lorrie Faith Cranor, The Cost of Reading Privacy Policies, https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf.

[51] https://plaid.com/legal/ios/#information-we-collect-and-categories-of-sources

[52] https://plaid.com/legal/ios/#information-we-collect-and-categories-of-sources

[53] "Plaid relies on a consent-based permissioned model, whereby consumers specifically authorize the sharing of financial accounts they select with the recipients they choose." https://www.banking.senate.gov/imo/media/doc/Data%20Submission_Plaid1.pdf

[54] See for example, Trim, Privacy Policy, Use of Plaid: *Trim uses Plaid Technologies, Inc. ("Plaid") to gather End User's data from financial institutions. By using our service, you grant Trim and Plaid the right, power, and authority to act on your behalf to access and transmit your personal and financial information from the relevant financial institution. You agree to your personal and financial information being transferred, stored, and processed by Plaid in accordance with the Plaid Privacy Policy.*, https://www.asktrim.com/privacy or in the case of Albert, Plaid's user agreement is three clicks away from the reference to it in Alberts' Terms of Use, Third Party Account Verification Provider, "Albert currently utilizes Plaid, a third-party technology company, to retrieve information from your linked bank account...For more information on Plaid, please see our Financial Data notice. https://albert.com/terms/. Albert's Financial Data Notice states, "In order for us to deliver the best service possible, we utilize technology developed by Plaid...For more on how Plaid collects and manages your information, please visit Plaid's privacy policy."https://albert.com/terms/plaid/ The click through from there takes users to Plaid's end user privacy policy: https://plaid.com/legal/#end-user-privacy-policy.

[55] For example, automated savings service Digit's privacy policy states that Digit "will hold your Personal Information for as long as we believe it will help us achieve our objectives." Accessing Your Information, https://digit.co/privacy.

or the potential for discrimination or abuse. For example, with the exception of insurance companies in very limited circumstances, financial services providers have no reason to collect or share consumer medical information;[56] and social media, including user generated content and contacts, should also be off limits.

**F. Legal requirements other than section 1033**

An area of regulatory uncertainty where the Bureau should take bold action is algorithmic accountability. Data collected about consumers is routinely processed by algorithms that make decisions about them. In financial services, algorithms are routinely used to determine auto insurance rates, creditworthiness, willingness to pay, and now as a result of the pandemic, we are seeing new ways in which consumer data is processed to assess people. For example, in addition to its FICO score used for credit decisioning, FICO now offers a "Resilience Index" which lenders can "leverage" to "rank-order consumers by sensitivity to economic stress."[57]

Proponents advocate for the use of artificial intelligence in financial services, claiming it can "reduce human biases and errors."[58] Algorithms are often positioned to consumers, regulators and financial institutions as expanding access to financial services[59] and/or decreasing bias in the provision or pricing of services.[60] For example, lender and bank service provider Upstart's mission "is to enable effortless credit based on true risk."[61] Upstart claims it uses "more than" 1,500 data points as part of its algorithmic decision making.[62] It also makes its Credit Decision API available to banks.[63] An analysis by the Student Borrower Protection Center (SBPC) raised questions about the fairness of Upstart's decision making.[64] For example, the SBPC reported that borrowers who refinance with Upstart may pay a penalty for having attended an historically black college or university.[65] (As a result, the company entered into a voluntary agreement with the NAACP Legal Defense and Educational Fund, Inc. SBPC "under which the parties will

---

[56] The bill negotiation and savings service Truebill's privacy policy allows Truebill the right to collect user health information: https://www.truebill.com/privacy.
[57] https://www.experian.com/consumer-information/fico-resilience-index
[58] Oliver Wyman, Insights Artificial Intelligence Applications in Financial Services, https://www.oliverwyman.com/our-expertise/insights/2019/dec/artificial-intelligence-applications-in-financial-services.html.
[59] See for example, LendUp: "We consider all types of credit history. Just because your credit score may be "not-so-great" doesn't mean you can't get approved." https://www.lendup.com/
[60] "Artificial intelligence (AI) presents an opportunity to transform how we allocate credit and risk, and to create fairer, more inclusive systems." Aaron Klein, Brookings Institution, Reducing bias in AI-based financial services, https://www.brookings.edu/research/reducing-bias-in-ai-based-financial-services/.
[61] https://www.upstart.com/about
[62] https://www.upstart.com/blog/introducing-credit-decision-api
[63] https://www.upstart.com/for-banks/credit-decision-api/
[64] Student Borrower Protection Center, Educational Redlining, https://protectborrowers.org/wp-content/uploads/2020/02/Education-Redlining-Report.pdf.
[65] *Id*. at 4.

collaborate on a review of Upstart's fair lending outcomes and assess best practices in the use and testing of alternative data in financial technology ("fintech") credit models."[66])

Claims of objectivity and proof notwithstanding, algorithms can and sometimes do exacerbate bias or have unexpected discriminatory effects, as numerous examples have demonstrated.[67] While there are laws that prohibit discrimination, there are not laws in place that ensure sufficient transparency, testing or accountability of algorithms. As consumers lack any means to correct erroneous conclusions made by algorithms, or any recourse to object to the use of an untested and undisclosed algorithm to make inferences or decisions about them, rules governing their use are needed. CR has specific suggestions for improving algorithmic accountability, including the following:

- **The use of algorithms should be transparent to the end users.** When algorithms make decisions about consumers the individual should have notice that an algorithm was used.
- **Algorithmic decision-making should be testable for errors and bias.** Algorithms should be able to be tested by outside researchers and investigators.
- **Algorithms should be designed with fairness and accuracy in mind.** Companies should not simply rely on outsiders to detect problems with their algorithms; instead, companies should be required to plan for and design to avoid adverse consequences at all stages of the development of algorithms.
- **The data set used for algorithmic decision-making should avoid the use of proxies.** Algorithms can only serve to address the question posed to them. When possible, algorithms should avoid the use of unnecessary proxies like zip codes, education data, or marital status as these can also serve as proxies for prohibited factors such as race.
- **Algorithmic decision-making processes that could have significant consumer consequences should be explainable.** In some cases, algorithms are programmed to learn or evolve over time, such that a developer might not know why certain inputs lead to certain results. This could lead to unfair results if there is no meaningful accountability for how decisions are made. If an algorithm is (1) used for a significant purpose, like the determination of a credit score and (2) cannot be sufficiently explained, then the process should not be used.[68]

---

66 https://www.naacpldf.org/press-release/naacp-legal-defense-and-educational-fund-and-student-borrower-protection-center-announce-fair-lending-testing-agreement-with-upstart-network/

67 ProPublica and Consumer Reports: Auto Insurers Charging Higher Rates in Some Minority Neighborhoods, First-of-its-kind analysis finds pricing disparities between minority and non-minority neighborhoods cannot be explained by average risks, suggests potential redlining, https://www.consumerreports.org/media-room/press-releases/2017/04/propublica_and_consumer_reports_auto_insurers_charging_higher_rates_in_some_minority_neighborhoods11/.

68 Justin Brookman, Katie McInnis, Re: Post-Hearing Comments on Algorithms, Artificial Intelligence, and Predictive Analytics for the Federal Trade Commission's Hearings on Competition and Consumer

If regulators fail to enact sufficient safeguards around the use of algorithms, artificial intelligence and machine learning, the risk is that these systems will perpetuate and further entrench existing inequities and biases.[69] The Bureau should use its UDAAP authority to and include in its 1033 rulemaking rules for algorithmic decision making in financial services to further consumer harm from unaccountable algorithmus.

**G. Data security**

The Gramm-Leach-Bliley Act (GLBA) makes a distinction between financial and other types of data. When the name of your first pet can be the key to account access, and money can be sent using only a phone number, the line between sensitive financial data and everything else is either already meaningless or well on its way to becoming so.

The Gramm-Leach-Bliley Act should not be mistaken for a privacy law. GLBA requires financial services providers to explain their information-sharing practices to their customers and to protect sensitive data.[70] The disclosures required by 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. Moreover, GLBA does nothing to curb data collection in excess of what is reasonably necessary. Its incentives to protect consumer data from unauthorized disclosure remain inadequate. Still, banks and financial services providers seek and get broad exemptions from state privacy laws by claiming that GLBA protects consumer privacy.[71] The GLBA regime does no such thing.

The Bureau can patch some of the gaping holes in GLBA by moving forward with rules that create a strong floor of protections for consumers and require data minimization, clear information about data practices, and strong data security practices. Rules should also include strong enforcement tools to ensure accountability.

**H. Data accuracy**

Many digital financial services applications are only as good as the accuracy of the data that drives them.  A credit score app that shows an inaccurate credit score is of little use to someone

---

Protection in the 21st Century on November 13-14, 2018, FTC-2018-0101, *available at* https://advocacy.consumerreports.org/wp-content/uploads/2019/02/CR-AI-FTC-comments.pdf.

[69] Kristin Johnson, Frank Pasquale, and Jennifer Chapman, Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation, 88 Fordham L. Rev. 499 (2019). Available at: https://ir.lawnet.fordham.edu/flr/vol88/iss2/5.

[70] Pub. L. 106-102

[71] For a discussion of the gaps and ambiguities in the California Consumer Privacy Act created by the GLBA exemption, see *The 2018 California Consumer Privacy Act: Understanding Its Implications and Ambiguities*, https://www.frbsf.org/banking/files/Fintech-Edge-Special-Report_CCPA.pdf at 5.

looking to secure credit on the best terms.[72] As noted above, some data permissioning practices can introduce inaccuracies. Consumers have little ability to assess the accuracy of the information that drives many digital financial apps because service providers don't make it available to them.

There are some instances where inaccurate data can be particularly harmful. Inaccurate consumer data on credit reports can negatively impact credit scores, which in turn affect people's ability to rent property, take out loans, insurance rates and even their ability to gain employment. Credit scores are a gatekeeper for accessing many of these basic services. These traditional data sources have clear consumer rights of review and correction, although it can be difficult for consumers to have inaccurate data corrected. There is increasing emphasis on the use of "alternative" data for underwriting. These models claim that they can be more inclusive of those who historically have been "credit invisible." This data can include information that has not traditionally been included on credit reports, such as social media activity, internet browser history, utility bill or telecom payments, and educational background.[73] Companies making these evaluations may be pulling information from datasets that might be incomplete or non-inclusive.[74] Under the Fair Credit Reporting Act (FCRA), the credit reporting agency and the information provider are responsible for correcting errors on a consumer report. Credit bureaus must provide the individual with a copy of their report when requested once every 12 months.[75] The FCRA applies to data collected for credit, insurance or employment purposes, and as such applies to both traditional credit bureaus and the newer service providers claiming to qualify people for credit using alternative data.

There are a number of open questions about if, when and how the FCRA applies to digital financial services, including whether and under what conditions data aggregators and other new intermediaries qualify as consumer reporting agencies, and whether and under what conditions their data sources are "furnishers" under FCRA requirements; whether notice and consent is adequate to secure consumer privacy rights; and if and how FCRA accuracy and dispute resolution requirements should be adjusted for data aggregators and their data sources given differences in their operations from traditional consumer reporting agencies and furnishers.[76]

At present, consumers may not, as discussed above, understand the role data aggregators play in digital financial services. And as also noted above, data aggregators may collect more information than is needed for particular purposes and the practice of adding/permissioning data access, under some circumstances, may itself introduce inaccuracies. Therefore we urge several solutions: mandated data minimization, securing consumer consent for each data

---

[72] This was the subject of a viral Tweet January 26, 2021: https://twitter.com/jjasshole/status/1353764543504248837?s=20

[73] https://www.gao.gov/assets/700/696149.pdf

[74] https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1122&context=yjolt

[75] https://www.consumer.ftc.gov/articles/0151-disputing-errors-credit-reports

[76] https://finreglab.org/cash-flow-data-in-underwriting-credit/consumer-financial-data-legal-and-regulatory-landscape-working-paper/ at viii.

collector/processor, and FCRA rights to information data aggregators have for consumers who are permissioning data access for FCRA purposes. We note that it is essential that if these recommendations result in separate systems for FCRA and non-FCRA rights, that rules do not undermine FCRA coverage. We agree with the National Consumer Law Center's Chi Chi Wu:

> If there is a controversy as to whether certain data qualifies as a "consumer report," any regulation should explicitly provide 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 most critically, it allows consumers the ability to protect themselves with access to the court system.

We further believe that the Bureau should fill gaps left by FCRA by mandating data minimization for all use cases; ensuring all service providers are required to give consumers the right to review and correct information financial service providers collect about them. Consumers also need a right the FCRA does not have: the right to demand deletion of accurate data about them when they leave a service.

**I. Other information**

Digital financial service providers make it far too difficult for consumers to contact them when they need help. CR has documented instances where consumers cannot effectively use the digital tools providers give them to resolve issues, and service providers fail to offer a telephone point of contact.[77] We urge the Bureau to consider ways in which it can incentivize providers to ensure that consumers can secure help quickly when their money is at stake.

**Conclusion**

While financial data sharing may give consumers a clearer picture of their financial condition, it also poses risks. Some of these risks are not yet accounted for in existing legal frameworks. We urge the Bureau to act to establish clear rules for consumer access to financial records to ensure consumer safety.

Sincerely,

Christina Tetreault
Manager, financial policy

[77] https://www.consumerreports.org/financial-planning/hidden-risks-of-online-savings-tools/