February 12, 2020

Kathy Kraninger
Director
Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552

Re: The Consumer Financial Protection Bureau's Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act

Dear Director Kraninger:

Thank you for inviting Consumer Reports (CR) to participate in the Consumer Financial Protection Bureau's Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act. Consumer Reports is an expert, independent, non-profit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves.[1] We appreciate the opportunity to share our perspective on this important topic.

Digital innovation brings many benefits to consumers. However, digital financial services -- with its prevalent and expansive collection, monetization, and use of personal consumer data -- can come into conflict with the right to privacy. Some data collection is necessary and appropriate, but often digital financial data collection far exceeds this baseline. A lack of transparency about data collection, use, and sharing practices, combined with that fact that consumers rarely read policies blurs the line between what is permissioned sharing and what is not. Consumers worry about privacy and security,[2] and those worries likely will not abate until the open questions regarding consumer rights are resolved. Industry efforts to ensure consumer access and control

[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.

[2] 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/.

are laudable, but alone are not enough. The Bureau should create clear rules for safe and accurate data sharing, and ensure vigorous enforcement to prevent misuse of consumer information.

Obtuse Privacy Policies Fail to Convey Scope of Consumer Data Collection and Sharing

Provider privacy policies across industries lack transparency.[3] 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,[4] and their agreements reserved broad rights to collect and share data for unrelated purposes, including targeted advertising.[5] 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,[6] are so confusing that consumers are unlikely to exercise their rights.[7]

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.[8] 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 39 different agreements in its Disclosure Library,[9] including two different privacy disclosures.[10] It is simply not efficient for consumers to read disclosures; a study by Aleecia McDonald and Lorrie

---

[3] 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/.

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

[5] 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/

[6] 15 U.S.C § 6802(b).

[7] *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.

[8] 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.

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

[10] RHF Privacy, https://cdn.robinhood.com/assets/robinhood/legal/RHF%20Privacy.pdf and Robinhood Financial Privacy and Security Policy, https://cdn.robinhood.com/assets/robinhood/legal/RHF%20Privacy%20and%20Security.pdf.

Cranor estimated that 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.[11]

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. If consumers did read them, 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."[12] While Plaid's terms state that while user data is not sold, it is shared.[13] Plaid claims user information is not shared without the user's "consent."[14] 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?[15]

Screen-scraping Creates Risks Outside Established Legal Frameworks

Screen-scraping is the practice in which users share their login credentials—usually username and passwords—in order to connect their accounts. All manner of financial services may rely on screen-scraping for data sharing, 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.[16] As the Bureau itself has reported, there

---

[11] 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.

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

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

[14] "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

[15] 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.

[16] See for example these findings from the Consumer Financial Protection Bureau report, Consumer-authorized financial data sharing and aggregation Stakeholder insights that inform the Consumer Protection Principles: This on security, at 7: "...many stakeholders agree that viable forms of access exist that are more secure than those that require consumers to share account credentials with third parties." and this on accuracy, at 9: "Many stakeholders acknowledge that screen scraping algorithms may be at greater risk of missing or misinterpreting data fields than sharing processes in which

is not a clear legal framework that accounts for risks associated with screen-scraping.[17] Several years ago, banks tried to make consumers liable for fraud on their accounts if they shared their account credentials.[18] CR research has found several services reliant on screen-scraping that put users on the hook for any losses associated with "use of or access to" their services.[19] The banks that consumers link to their accounts, the data aggregators that these services rely on for that linkage, and these services themselves are rich targets for hackers.[20] It seems only a matter of when, not a matter of if, these policies will be tested.

Industry Efforts to Create Consumer Controls Are Good but Alone Are Not Enough

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. The Digital Standard lays out best consumer privacy and security practices.[21] Some of these best practices include data minimization, reasonable measures to keep consumer data secure, and easy-to-use, standardized tools that give consumers control over their information and allow them to stop companies from using their data for extraneous purposes. CR supports and is working on efforts to make these types of controls the industry standard in financial services, and has joined Financial Data Exchange (FDX) to that end.[22] However, consumers

---

account data holders transmit data to account data users or aggregators through direct data feeds." https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf

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

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

[19] 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…" 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#your-use-of-the-service 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

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

[21] *The Standard*, The Digital Standard, https://www.thedigitalstandard.org/the-standard (last visited Feb. 8, 2020).

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

shouldn't bear the entire burden of protecting their privacy through settings and controls. There needs to be a strong backstop in law to ensure consumer privacy, security and safety.

The Bureau Should Ensure Consumer Protection by Establishing Clear Rules of the Road

In 2017, the Bureau published its Consumer Protection Principles: Consumer–Authorized Financial Data Sharing and Aggregation.[23] These principles contain best practices, but as noted above, best practices alone are not enough. Consumers need strong protection under law. Specifically, there is an urgent need for a comprehensive legal framework that clearly establishes consumer rights and remedies in the event of unauthorized access, inaccurate information, or other fraud or error as a result of data sharing.

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,[24] 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 or the potential for discrimination or abuse. For example, with the exception of insurance companies vetting customers, financial services providers have no reason to collect or share consumer medical information;[25] and social media, including user generated content and contacts, should not be allowed for credit decisioning. We further suggest that consumers have the right to safely, quickly and easily port their account information, including account numbers, from one service provider to another. This will ensure robust competition and prevent consumers from being "trapped" at a particular financial service provider.[26]

---

[23] *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.
[24] 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.
[25] The bill negotiation and savings service Truebill's privacy policy allows Truebill the right to collect user health information: https://www.truebill.com/privacy.
[26] 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/.

Conclusion

Thank you for hosting the Symposium on Consumer Access to Financial Records, Section 1033 of the Dodd-Frank Act, and for the opportunity to participate. 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.

Christina Tetreault
Senior Policy Counsel
Consumer Reports