COMMENT OF THE FINANCIAL HEALTH NETWORK

ADVANCE NOTICE OF PROPOSED RULEMAKING
PERSONAL FINANCIAL DATA RIGHTS RECONSIDERATION
Docket No, CFPB-2025-0037

The Financial Health Network appreciates this opportunity to comment on the CFPB's Advance Notice of Proposed Rulemaking (ANPR) on "Personal Financial Data Rights Reconsideration" issued pursuant to § 1033 of the Dodd-Frank Act.

Interest of the Financial Health Network

The Financial Health Network (FHN) is a non-profit organization that unites business leaders, policymakers, and innovators in a shared mission to improve financial health for all. As a membership organization, FHN includes among its members both "data providers" and "authorized third parties" as defined in the 2024 Personal Financial Data Rights Rule (PFDR Rule or the Rule). Moreover, FHN itself would qualify as a third party because, as part of its ongoing research program to better understand and measure financial health, FHN, with the permission of respondents to FHN's annual Financial Health Pulse survey, has accessed respondents' transactional data and linked those data to their survey responses to provide more robust insights into the financial health challenges Americans face.[1] And, through its Financial Solutions Lab, FHN has invested in and nurtured several innovative financial technology companies that rely on consumer-permissioned financial data to deliver services designed to help consumers advance their financial well-being. All of these perspectives inform this comment.

Because of the significant role that personal financial data rights can play in building the scaffolding for products and services that will advance consumers' financial health and in enabling research to better understand the state of financial health, FHN has been actively engaged with the issues raised by § 1033 for the past decade. In 2016, we issued the first set of principles to "guide the financial services industry as it works to establish a data-sharing ecosystem that is secure, inclusive and innovative."[2] The following year, in a follow-on report, FHN put forward more detailed recommendations regarding issues of liability, transparency, and consumer control and issued a "call to action for financial service providers and regulators."[3]

---

[1] For an overview of the Financial Health Pulse, *see* *https://finhealthnetwork.org/programs/financialhealth-pulse/*. The Pulse Points available there illustrate how FHN has used survey and transactional data in our research.
[2] CFSI's Consumer Data Sharing Principles. At the time these Principles were issued FHN was known as the Center for Financial Services Innovation (CFSI).
[3] Liability, Transparency, and Consumer Control in Data Sharing

Since 2017, we have published several widely-cited research reports and opinion pieces on this topic.[4] And, FHN has participated in all stages of the PFDR rulemaking, from the 2020 Symposium on Consumer Access to Financial Records at which we were invited to participate as a panelist,[5] through comments submitted in response to the 2020 Advance Notice of Proposed Rulemaking, the 2022 SBREFA Outline of Proposals and Alternatives Under Consideration, and the 2023 Notice of Proposed Rulemaking. FHN also unsuccessfully sought leave to file a brief *amicus curiae* in the Bank Policy Institute's challenge to the PFDR Rule.

Summary of the Financial Health Network's Comment

This Comment addresses the following issues:

Scope of Who May Make a Request on Behalf of a Consumer: The PFDR Rule imposes on "authorized representatives" a set of duties that, in some respects, are more demanding, and in other respects less demanding, than the requirements that are imposed on fiduciaries under the common law of agency. This is both a lawful exercise of the CFPB's rulemaking authority and a resolution well calibrated to achieve a secure, well-functioning data sharing ecosystem. Limiting data access to authorized representatives who assume fiduciary responsibilities would disserve those interests and would be inconsistent with the statutory language, with the way that "authorized representative" has been interpreted by the CFPB in the context of handling consumer complaints, with the way the words "agent" and "representative" are used in the Dodd-Frank Act, and with the way that data sharing was working when the Act was enacted..

Defrayment of Costs in Exercising Rights Under Section 1033: By requiring data providers to "make available to a consumer, *upon request,*" the consumer's personal financial data, Congress in § 1033 precluded data providers from conditioning consumers' data access upon their payment of a fee. It is thus for Congress to decide whether to permit data providers to charge a data access fee or whether data providers should be expected to recover the costs of providing data access through the pricing of the accounts to which data access is allowed (including the interest rate spread on deposits), just as costs for other features of checking and credit card accounts are recovered. If the CFPB were to disagree, it should, at a minimum, place guardrails on fee assessments to limit such fees to those reasonably calculated to recover the variable costs of providing data access rather than allowing banks to set fees, or even negotiate fees, that hinder competition among banks or among aggregators.

Information Security Concerns in the Exercise of Section 1033 Rights: The PFDR Rule establishes the core principles required to protect information security by placing obligations on

[4] *E.g.,* Financial Data: The Consumer Perspective (2021); Consumer Financial Data: Legal and Regulatory Landscape (2020); Silberman & Stone, CFPB Should Write a Data Sharing Rule That Can Evolve With the Market (American Banker, August 3, 2022); Tescher, Stone & Silberman, The Open Banking Rule Helps Consumers. Why Are Banks Against It? (American Banker, Dec. 13, 2024); Teacher & Silberman, Open Banking Fees Threaten Financial Health (Open Banker, October 7, 2025).

[5] *See* Statement of Dan Murphy, *available at* https://files.consumerfinance.gov/f/documents/cfpb_murphy-statement_symposium-consumer-access-financial-records.pdf

authorized third parties with respect to their information security practices and by permitting data providers to deny access to data based upon reasonable concerns with respect to a particular third party's information security. The CFPB should not attempt to be more prescriptive in this regard but rather should leave it to the market, through the development of consensus standards and certification processes, to particularize and implement these principle-based requirements.

Privacy Concerns in the Exercise of Section 1033 Rights: The authorization and reauthorization procedures set forth in the PFDR Rule, the requirement that authorized representatives obtain only those data elements reasonably necessary to deliver the product or service the consumer has requested from the third party, and the further prohibition against the sharing of the consumer's data with (unauthorized) third parties are generally well-calibrated to protect consumers' privacy interests. However, the limitation the Rule places on the ability of an authorized representative to use data which the representative has been authorized to obtain for product development purposes, as well as the limitation the Rule places on sharing deidentified data with academics and other bona fide researchers, are not necessary to protect consumers' privacy and will have unintended consequences in limiting both product innovation and consumer finance research. If the CFPB elects to issue a proposed rule amending the PFDR Rule, the Bureau should propose modifications to these provisions.

I. Who May Make a Request on Behalf of an Individual Consumer

To address the questions posed in the first section of the ANPR, some background regarding the evolution of "open banking"–the term that is generally used to refer to the ecosystem that has evolved for the sharing of consumer-permissioned financial data–is needed.

Open banking had its genesis in the United States in a set of technological and market developments in the late 1990s. In January, 1997, Microsoft, Intuit, and CheckFree announced that they were "creating a single, unified technical specification, called Open Financial Exchange, that will enable financial institutions to exchange financial data over the Internet" in order to "accelerate the adoption of electronic financial connectivity."[6] Two years later, a company named Yodlee was founded and introduced what it termed the "first digital aggregation product to the digital financial services industry;"[7] that product enabled Yodlee to use a consumer's log-In credentials for one or more accounts (i.e., their username(s) and password(s)) to log into those accounts, capture the information or images displayed on the consumer's account portal(s) through a process known as "screen scraping," and convert that content into standardized, machine-readable data.

These products quickly gained market traction as several large banks, including Citibank, Wells Fargo, and JP Morgan Chase, elected to offer their customers–and in some cases non-

[6] Intuit, Microsoft, and CheckFree Create Open Financial Exchange. In 2019, the Open Financial Exchange (OFX) joined the Financial Data Exchange (FDX) and FDX took over management of the OFX protocol.

[7] Yodlee, Inc. Form S-1 Registration Statement at p.94, https://www.sec.gov/Archives/edgar/data/1161315/000095012314003249/filename1.htm#toc684206_4

customers–the ability to bring together in a single site information regarding all their financial accounts by permissioning the bank (working through Yodlee or some other aggregator) to access their account data.[8] By 2001, the Office of the Comptroller of Currency deemed it advisable to provide guidance to banks regarding the offering of "bank account aggregation services."[9] And before the end of the decade, fintechs like Mint.com were competing with incumbent financial institutions in offering account aggregation and related personal financial management services.[10]

Adding to the momentum, in 2008 Richard Thaler and Cass Sunstein published their influential book, *Nudge,* in which they argued that consumers should be deemed to own transactional data from their accounts and that those data should be accessible in a machine-readable format. Thaler and Sunstein envisioned a future in which what they termed "decision engines" could ingest such data and help a consumer shop for products, such as credit cards or mobile phone services, which would have the lowest net cost for that consumer given the consumer's usage pattern as revealed by the consumer's transactional history.

It was against this background that Congress in the Consumer Financial Protection Act of 2010 (CFPA)--Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act–enacted § 1033, thereby enshrining into the corpus of consumer financial protection law a provision that imposes a legal duty on "covered persons," and creates a correlative right in consumers, with respect to the sharing of consumer financial data. Specifically, CFPA § 1033 requires covered persons–defined to mean "any person that engages in offering or providing a consumer financial product or service," CFPA § 1002(6), 12 U.S.C. § 5481(6)--to "make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person." And, in marked contrast to all other federal consumer financial protection laws which define the word "consumer" to mean only an "individual" or a "natural person,"[11] Congress in the CFPA defined consumer more broadly to mean both "an individual" and also "an agent, trustee, or representative acting on behalf of an individual." *Id.* § 1002(4), 12 U.S.C. § 5481(4).

From the first, the CFPB has understood the phrase "representative acting on behalf of an individual" to encompass anyone acting at the request of an individual. On this basis the CFPB's process for "the centralized collection of, monitoring of, and response to *consumer* complaints" —a process required by § 1013(b)(3) and § 1034 of the CFPA, 12 U.S.C. §§ 5493(b)(3), 5534— has been open and responsive not only to complaints filed by an aggrieved individual but also to complaints filed on behalf of such an individual by someone the consumer authorized or requested to do so, including both attorneys who owe a fiduciary duty to the aggrieved individual

[8] Citibank's Aggregation Portal a Big Draw (Computer World, September 18, 2000).
[9] OCC Bulletin 2001-12 (Feb. 28, 2001).
[10] Mint launched in September 2007 and, after two years of rapid growth, was purchased by Intuit which eventually merged Mint into Credit Karma which Intuit also purchased. Ahshan, Postmortem: Did Intuit Kill Mint or Was PFM Already on Life Support? (Tearsheet, Nov. 22,2023).
[11] Truth in Lending Act, 15 U.S.C. § 11602(i)(natural person); Credit Repair Organization Act, 15 U.S.C. § 1679a(1) (individual); Electronic Funds Transfer Act, 15 U.S.C. § 1693a(6) (natural person); Fair Credit Reporting Act, 15 U.S.C. § 1681(c)(individual); Fair Debt Collection Practices Act, 15 U.S.C. § 1692a(3)(natural person).

and lay representatives, such as friends or family members, with no such duty.[12] (Any decision in the PFDR rulemaking to limit the interpretation of "consumer" to cover only representatives acting in a fiduciary capacity thus would necessarily narrow access to the consumer response function and complicate the administration of the consumer response system.)

The understanding of the word "representative" adopted by the Bureau in the consumer response context accords with that word's plain meaning, as the dictionary defines representative to mean "one who stands for or acts on behalf of another."[13] And, this understanding accords as well with the way in which the word "representative" is used throughout the CFPA–and the other titles of the Dodd-Frank Act as well–to cover both those acting in a fiduciary capacity as a legal representative as well as non-fiduciary lay representatives. This is true both of provisions using only the word "representative,"[14] and of multiple provisions in which the word "representative" appears as one of a series of nouns in a context in which it is unlikely that the other words in the series were intended to narrow the meaning of the word "representative."[15] Indeed, in several places in the Dodd-Frank Act Congress used the phrase "legal representative" when it sought to delimit the scope of the word "representative."[16]

---

[12] *See, e.g.,* 76 Fed. Reg. 76628, 76631 (Dec. 11, 2011) (proposed policy on disclosure of complaints); 77 Fed. Reg. 37558, 37567 (June 12, 2012) (final policy on disclosure of complaints).

[13] Black's Law Dictionary (12th ed. 2024); *see also* Merriam-Webster ("someone who represents another as agent, deputy, substitute or delegate").

[14] *E.g.,* CFPA. § 1014 (Consumer Advisory Board shall include "representatives of depository institutions"); *id.* § 1017(a)(5)(A) ("representatives of the Government Accountability Office shall have access" to the personnel and books and records of CFPB); *id.* § 1025(e)(4)(B) (panel hearing appeals of supervisory determination shall be composed of "a representative from the Bureau," a representative of the prudential regulator" bringing the appeal, and "one individual representative" from one of the other prudential regulators). The other titles of the Dodd-Frank Act are replete with provisions using the word "representative" in this manner.

[15] For example, CFPA § 1012(b), 12 U.S.C. § 5492(b) authorizes the Director to delegate authority to "any duly authorized, employee, representative, or agent"); CFPA § 1027(I)(1), 12 U.S.C. § 5517(I)(1) precludes the CFPB from exercising jurisdiction over "any agent, volunteer, or representative" soliciting contributions to a tax-exempt organization; and CFPA § 1057(a), 12 U.S.C. § 5567(a) prohibits covered persons from retaliating against any "employee or any authorized representative" for asserting rights under federal consumer financial protection law. These provisions undoubtedly cover both attorney and lay representatives. Similarly, outside of the CFPA, Dodd-Frank Act § 122(b)(1)(C), 12 U.S.C.§ 5332(b)(1)(C), grants the Comptroller General, in conducting certain audits, a right of access to "the Officers, directors, employees, financial advisors, staff, working groups, and agents and representatives" of the body being audited, and § 989(d), 124 Stat. 1941, grants the Comptroller General, in conducting a prescribed study, access to the books and records of certain entities and their "officers, directors, employees, independent public accountants, financial advisors, staff, and agents and representatives." These provisions, too, would seem to cover both attorney-fiduciary and non-attorney representatives

[16] Dodd Frank Act § 913(a),(g)(2), 124 Stat. 1824, 1829 ("'retail customer' means a natural person or the legal representative of such natural person); Dodd-Frank Act § 748, 124 Stat. 1741 (amending the Commodity Exchange Act to add as § 23(c)(B)(II) authorization for whistleblower fee awards based in part on "the degree of assistance provided by the whistleblower and any legal representative"); Dodd-Frank Act § 922, 124 Stat. 1842 (amending the Securities Exchange Act of 1934 to add as § 21F(c)(i)(II) authorization for whistleblower fee awards based in part on "the degree of assistance provided by the whistleblower and any legal representative").

It is, of course, true that in § 1002(4), the phrase "representative acting on behalf of an individual" is preceded by the words "agent" and "trustee." That has given rise to the question posed by the ANPR as to whether "'representative" in this definition "is intended to encompass only those representatives that are serving in a fiduciary capacity" (Question #3) and the further question as to the extent to which such an interpretation would "limit customers' ability to transfer their transaction data to third parties under section 1033 or the ability of financial technology and other third-party service providers to compete with incumbent market participants" (Question #5).

The implicit premises of the first of these questions seem to be that the word "agent" inexorably refers to one acting in a "fiduciary capacity" and that there is a clear line of demarcation between such fiduciary relationships and other types of relationships. But as the Restatement of Agency states, "the terminology of agency is widely used in commercial settings…to characterize relationships that are not necessarily encompassed by the legal definition of agency"–which carries with it fiduciary obligations–as it is "common usage to refer without distinction to parties who serve any intermediary function as "agents."[17] Indeed, the Dodd-Frank Act itself frequently uses the word "agent" as part of a series of terms in contexts which indicate that the word is not intended to be used as a legal term of art limited to those with a fiduciary duty but rather encompasses both fiduciaries and non-fiduciaries acting in an intermediary or representative capacity.[18] Other federal laws likewise use the word "agent" in the sense of an intermediary.[19] Thus, the fact that the word "representative" in the CFPA's definition of "consumer" is preceded by the word "agent" does not, in and of itself, justify deviating from the plain meaning of "representative" to imply a fiduciary limitation.

At the same time, because the term "agent" is used in contexts that do not necessarily denote legal agency with attendant fiduciary duties, interpreting the phrase "representative acting on behalf of an individual" in the CFPA's definition of "consumer" to refer only to those with fiduciary duties would create a myriad of practical problems in the context of § 1033, problems that would negatively impact the ability of consumers to permission access to their data. Under such an interpretation, a consumer desiring to authorize a third party to obtain some of the consumer's financial data, in order to obtain a service from that third party, would have to first determine whether the third party owes, or would owe, a fiduciary duty to the consumer under whatever state or federal law governs the relationship. Similarly, a covered person called upon to share data with an authorized third party would have to assess the third party's fiduciary status to determine whether § 1033 applies. (The same would be true for the CFPB itself in determining whether to accept a complaint submitted on behalf of an aggrieved individual under CFPA § 1034.)

---

[17] Restatement (3d) of Agency § 101 Comment (b).

[18] In several of the statutory provisions cited in n.15, the word "agent" is used along with the word "representative" in contexts indicating that neither is intended to refer only to fiduciaries. Similarly, § 122(j)(2), 124 Stat. provides for expedited consideration of cases brought by the FDIC against "a director, officer, employee, agent, attorney, accountant, or appraiser"; again it seems unlikely that the word "agent" is intended in a limited sense.

[19] For example, regulations issued by the IRS state that for purposes of the Internal Revenue Code, "the word agent does not denote a fiduciary." 26 C.F.R. § 401.7701-6.

Moreover, the law of agency recognizes that "the legal consequences of agency"–that is, the fiduciary duty to a principal that agency law imposes on those who meet the legal definition of agent–"may attach to only a portion of the relationship between two persons."[20] That adds to the complexity that would arise if the phrase "representative acting on behalf of an individual" were interpreted to mean one acting in a fiduciary capacity on behalf of an individual as, under such an interpretation, to assess whether the third party is acting in a fiduciary capacity would require parsing the relationship between the individual and the third party to determine which aspects of the relationship are governed by a fiduciary duty.

At the same time, the fact that a fiduciary duty can attach to aspects of a relationship suggests that a "representative" can owe certain fiduciary duties to a consumer in procuring data at the consumer's behest–that is, function as a "data fiduciary" as one commenter has put it –even if the overall relationship between the parties is more arm's length in nature.[21] Indeed, although the PFDR Rule does not limit the term "representative" to those with a preexisting fiduciary duty under state or federal law, the Rule does impose on a third party seeking to qualify as an "authorized third party" a set of duties designed, as the Bureau explained, to "ensure that the third party is accessing data as a representative acting on behalf of the consumer." 89 Fed. Reg. at 90930. Those duties–adopted pursuant to the Bureau's broad rulemaking authority under § 1033 as well as § 1022(b)(1)–in substance, require an authorized third party to act like a "data fiduciary."[22]

For example, § 1033.411(b) of the PFDR Rule requires a third party, in order to qualify as an "authorized third party," to agree to collect only those data elements that "are reasonably necessary" to deliver the "consumer's requested product or service" and to use those data only for that purpose, and § 1033.421(a) in turn requires authorized third parties to abide by those limitations. Similarly, PFDR § 1033.421(a)(2)(ii) and (f) prohibit an "authorized third party" from selling the consumer's data to a third party or from sharing the data with another party except as needed to deliver to the consumer the requested product or service. As the Bureau stated, "Where third parties seek to use data to advance their own interests, rather than to act for the consumer, such action would not be on behalf of the consumer." 89 Fed. Reg. at 90932-33. These provisions parallel core elements of the duties that an agent owes to a principal under common law, including, e.g., the duty to adhere to the scope of the agent's actual authority, to preserve the confidentiality of information belonging to the principal, and, more generally, to act for the benefit of the principal rather than to further the agent's self-interest.[23]

---

[20] Restatement (3d) of Agency § 101 Comment (b).

[21] Johnson, *A Field Guide to the Next Round of Open Banking Fights* (Fintech Takes, August 22, 2025).

[22] Under § 1033(a), the duty of covered persons to provide data to consumers is "subject to rules prescribed by the Bureau"; it is because the duty is dependent on rulemaking that § 1033 has not been understood to be self-executing. Thus, the Bureau's rulemaking authority under § 1033 goes far beyond the instruction in subsection (d) to issue a rule to "prescribe standards…to promote the development and use of standardized formation for information." More generally, § 1022(b)(1) grants the CFPB broad authority to "prescribe rules…as may be necessary or appropriate to enable the Bureau to administer and carry out the purposes and objectives of the Federal consumer financial laws," including the CFPA..

[23] Restatement (3d) of Agency §§ 805, 809.

Indeed, in certain respects the duties that the PFDR Rule imposes on authorized third parties go beyond anything that would be required under fiduciary law. To begin with, under § 1033.421(b)(2), an authorized third party's authorization to collect data expires every twelve months; there is no comparable provision in agency law that causes an agency's authority to lapse at periodic intervals unless expressly renewed. Similarly, § 1033.421(h) requires authorized third parties to provide consumers with "a method to revoke the third party's authorization to access the consumer's covered data that is as easy to access and operate as the initial authorization;" again, this requirement finds no comparable provision in agency law.

Perhaps most importantly, a core principle of agency law is that a principal can, by contract, release an agent from any of the duties of loyalty otherwise required of the agent as a fiduciary.[24] Thus, for example, under agency law an agent could access data that it did not need to serve the consumer and could sell those data to a third party for the agent's own gain so long as the consumer had knowingly authorized such conduct. In contrast, the duties that the PFDR Rule imposes on authorized third parties, such as the duty to collect only those data elements needed to deliver a particular product or service to the individual and to use the data only for that purpose, cannot be waived. In an age in which consumers have become accustomed to scrolling through detailed terms and clicking an "I agree" button, this aspect of the Rule provides important protections to ensure that consumers' authorizations are truly knowing. As the CFPB stated in explaining its decision not to allow third parties to offer consumers the option to opt-in to various secondary uses:

> The CFPB is concerned that consumers might not receive adequate information through granular choice mechanisms that would result in meaningful consent. The CFPB is also concerned that if offered too many opt-in choices in the course of a single-authorization process, consumers might experience decision fatigue or choice paralysis, and therefore might agree to terms they have not considered…[89 Fed. Reg. at 90941]

At the same time, the PFDR Rule allows a third party to use data obtained with the consumer's authorization in certain ways that may or may not be consistent with the fiduciary duties that an agent owes to a principal at common law. For example, under agency law, absent a principal's consent, an agent has a duty "not to mingle the principal's property with anyone else's" and "not to use property of the principal for the agent's own purposes".[25] If these duties were imposed upon representatives under § 1033, it is unclear whether those representatives could, e.g., create a database of data obtained with the permission of multiple individuals and use those data for validating and refining existing models or for building new models to improve the product or services provided by these representatives. These uses are expressly permitted by the PFDR Rule without regard to whether each individual consumer whose data is so used stands to benefit from such uses on the ground that these are the types of uses that consumers reasonably expect when permissioning access to their data.[26] (As we discuss in Part IV, we believe that the list of

[24] *Id.* § 806.
[25] *Id.* §§ 805(1) and Comment (b), 812(2).
[26] *See* PFDR Rule § 1033.421(c); 89 Fed. Reg. at 90940.

permissible uses should be expanded in certain respects to facilitate both product innovations and empirical research.)

As the foregoing examples illustrate, the duties that the PFDR Rule imposes on authorized representatives–duties that create a "data fiduciary" type relationship–are generally well calibrated to facilitate the data sharing ecosystem that had begun to emerge at the time the CFPA was enacted and that Congress presumably intended to foster. That system has enabled innovations that have enhanced the efficiency and competitiveness of consumer finance markets and that have empowered Americans to advance their financial health. And that system would be severely threatened if only those acting in a fiduciary capacity under state or federal law could qualify as a "representative" for § 1033 purposes.

Consider, for example, person-to-person (P2P) payment apps, such as Venmo or CashApp. These apps have brought competition to the payment system and delivered real value to consumers by enabling consumers to send money to other members of the network in real time without having to wait for a check or ACH payment to settle and without having to maintain a cash balance in their P2P account. To offer this service, the apps typically obtain the consumers' authorization to access data with respect to the balance of a linked checking account so that, before sending a P2P payment as requested by the consumer, the app can, when it deems it necessary, verify that the app will be able to recover the payment from funds in the linked account.

Similarly and more broadly, consumer-permissioned access to account balance information facilitates both recurring and one-time "pull debit" transactions, as the party authorized by a consumer to pull a payment from the consumer's account–for example, a lender to whom a loan payment is due–can first verify that the account has the necessary funds to cover the payment before initiating the transaction. This use of the data spares the consumer from the risk, and potential cost, of an overdraft or NSF fee and saves the lender from the potential expense of a failed payment.

Or consider the use of consumer-permissioned data in the credit underwriting context. Since the advent of the national consumer reporting agencies (NCRAs) and credit scoring algorithms such as those offered by FICO, lenders generally have based credit decisions on credit scores generated from the information contained in consumer reports maintained by the NCRAs. But the information in those reports is generally limited to data furnished to the NCRAs by lenders with respect to loan payments and does not include payment history with respect to other types of recurring obligations, such as rent, utility, or telecommunications payments. That omission has disadvantaged the estimated 25 million Americans who do not have sufficient credit history to generate a credit score.[27] Further, even for consumers with a scorable credit history, their credit report provides at best an incomplete picture of their payment history and can provide an inaccurate picture especially where a consumer's current financial situation differs–for better or worse–from what was true in the past. Thus, for example, the credit score of a consumer who has

[27] Kambara & Luce, Technical correction and update to the CFPB's credit invisible estimate (CFPB 2025), This study finds that 12.5% of Americans lack a credit score; that translates to roughly 25 million individuals.

recovered from a past financial difficulty may understate that individual's current financial capability whereas the score of one who has recently encountered such a difficulty may overstate their current financial capacity.

Consumer-permissioned access to checking account data, coupled with advances in machine learning, have fueled multiple innovations to address these limitations of the credit reporting system–innovations that, as the Treasury Department recognized in its 2018 report on fintech and financial innovation, "have the potential to meaningfully expand access to credit and the quality of financial services."[28] For example, some apps, including an app offered by one of the NCRAs as well as multiple apps offered by fintechs, obtain a consumer's authorization to access transactional data from their checking account to identify recurring bill payments that are not included in traditional credit reports; these apps then furnish that information to the NCRAs so that the data can be incorporated into the consumer's credit report and used to generate, or enhance the predictiveness of, a consumer's credit score using credit scoring models built on both conventional credit bureau data and on these additional data sources.[29]

In a similar vein, for consumers applying for credit, many lenders–including both traditional financial institutions and online fintech lenders–now solicit consumers' authorization to access data from their checking account to engage in what has come to be called "cash flow underwriting." With such authorization, lenders can access data regarding cash inflows, outflows, balances, and bill payments which can then be used either to supplement or substitute for underwriting based on credit history and credit scores. Such cash flow underwriting has enabled some lenders to introduce new types of credit products—such as short-term, no-interest cash advances—in which the loan proceeds are directly deposited into the consumer's checking account and the loan payment debited from that account when due.[30] Other lenders use consumer-permissioned cash flow data to underwrite for more conventional credit products such as credit cards and auto and personal loans; indeed, since 2020, over three successive Administrations, the Office of the Comptroller of the Currency has been working with financial institutions to enhance financial inclusion through cash flow underwriting.[31] There are now multiple cash flow scores available in the market that lenders can use, along with consumer-permissioned data, for underwriting purposes and abundant evidence of the value of cash flow data in assessing consumers' creditworthiness.[32]

---

[28] U.S. Department of Treasury, A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech and Innovation at 20 (2018); *see also id.* At 7 ("New platforms for lending are developing business models that take advantage of new types of data and credit analysis, potentially serving consumer and small business borrower segments that may not otherwise have access to credit").

[29] Experian offers an app of the type described in text, *see https://www.experian.com/credit/score-boost/*; for a compendium of other such apps *see Cochran & Stegman, Utility, Telecommunications, and Rental Data in Underwriting Credit* (Urban Institute 2022).

[30] Examples include Dave ExtraCash, https://dave.com/about-extra-cash, Money Lion InstaCash, https://www.moneylion.com/cash-advance/instacash, and Earnin Cash Advance, https://www.earnin.com/

[31] *See, e.g.,* OCC, Project REACh Alternative Credit Assessment Workstream

[32] The available cash flow scores include one recently launched by Experian, https://www.experianplc.com/newsroom/press-releases/2025/launch-of-experian-s-cashflow-score-signals-new-era-of-open-bank and scores from Prism Data, https://prismdata.com/cashscore/, and Nova Credit, https://www.novacredit.com/novascore. Studies establishing the value of cash flow data include,

It is unlikely that any of these innovations would have been possible, or could continue, if data access were limited to representatives acting in a fiduciary capacity. Surely a lender authorized to access transactional data to consider a consumer's application for credit—or a lender authorized by an existing customer to access such data for ongoing account management purposes--does not stand in a fiduciary relationship vis-a-vis the applicant. The same is true with respect to a payee authorized to access account balance data before initiating a debit from the consumer's account including, e.g., a P2P app, a lender, or some other person to whom money is or will be owed.

Even the viability of personal financial management (PFM) apps would be threatened if data access were limited to representatives acting in a fiduciary capacity. As the Treasury Department's 2018 report observed, "Digital advice platforms are making financial planning tools and wealth management capabilities previously limited to higher net worth households available to a much broader segment of households."[33] These apps provide invaluable support to consumers in managing their increasingly complicated financial affairs and are especially helpful for those whose financial situation is precarious. For example, PFM apps can help consumers establish and adhere to a family budget; optimize the timing and amount of their bill payments; increase their savings; and avoid overspending their accounts. Some PFM apps simply provide information and advice and leave it to the consumer to act on that advice; others are authorized by the consumer to affect transactions on the consumer's behalf–for example, to move money into a savings account under defined circumstances. This is only likely to increase with the advent of agentic AI. The common denominator across all PFM apps–both those already existing and those likely to emerge with the growth of AI–is that they are dependent on transactional and account data, often across multiple accounts including checking, savings, and credit cards accounts, accessed on an ongoing basis with the consumer's authorization to deliver their advice and other services.[34]

It is unclear whether some or all of these different types of PFM apps owe a fiduciary duty to the consumers to whom they provide financial advice. The answer to that question may vary from state to state and from app to app depending on the specific types of services being provided and, potentially, on the financial arrangement between the consumer and the app. (Some apps are paid purely on a subscription basis; others may earn some of their revenue from transactions in which they engage on the consumer's behalf or on transactions that the consumer undertakes based on the advice received.) But precisely because of this ambiguity, a rule that limited data access to third parties acting in a fiduciary capacity would almost surely cause major disruption in the ability of PFM apps to continue to function.

FinReg Lab, Advancing the Credit Ecosystem: Machine Learning and Cash Flow Data in Consumer Underwriting (2025); FinReg Lab, The Use of Cash Flow Data in Underwriting Credit: Empirical Research Findings, Technical Report (2019), *;* Alexandrov, Brown & Jain, Looking (CFPB, 2023), Johnson, Everything(Fintech Takes, May 22, 2024).

[33] *A Financial System That Creates Economic Opportunities, supra* n.28, at 7.

[34] Examples of these PFM apps include You Need a Budget, Rocket Money, Cleo, and Opportun.

At the same time, because depository institutions do not owe a fiduciary duty to their customers vis-a-vis their customers' data, interpreting "representative" in § 1033 to cover only fiduciaries would create an unlevel and distorted playing field. Banks could, for example, engage in cash flow underwriting or provide financial advice so long as they based their decisions or advice solely on transactional data internal to the bank. This would benefit those with large customer bases and thus disadvantage those seeking to compete with large banks, including community banks, de novo banks, and fintechs. And, such an interpretation would discourage banks from seeking their customers' authorization to access data regarding external accounts in order to obtain a more complete and accurate picture of their customers' financial situation, as importing external, consumer-permissioned data would trigger fiduciary duties on the bank with respect to such data.

In its 2018 Report, the Treasury Department during the first Trump Administration recognized that "narrowly interpreting Section 1033 as applying only to direct consumer access would do little to advance consumer interests by eliminating many of the benefits they derive from data aggregation and the innovations that flow through from fintech applications."[35] As shown above, the same would be true of a narrow interpretation that applied only to individual consumers and representatives acting in a fiduciary capacity.

For all these reasons, the Financial Health Network urges the CFPB to adhere to the basic approach of the PFDR Rule–and the Bureau's prior interpretation in the consumer response context–with respect to the definition of "representative acting on behalf of an individual" and allow third parties that satisfy the Rule's requirements for an "authorized representative"–including the Rule's "data fiduciary" requirements–to access data with the consumer's authorization.

II. Can Data Providers Require Consumers to Pay a Fee to Access Their Data?

The second section of the ANPR states that § 1033 "is silent on the question of how the burden of consumers' exercise of the rights it creates should be shared between the consumer and the 'covered person'" and poses a set of questions based upon that premise. FHN respectfully disagrees with the premise.

Section 1033 states that a "covered person shall make available to a consumer, *upon request,* information in the control or possession of the covered person concerning the consumer financial or product that the consumer obtained from such covered person" That means that consumers have a statutory right to such data and that the only precondition for a consumer obtaining data regarding their account is making a request. If a covered person were to deny a consumer's request for data on the ground that the consumer had failed to pay a fee, the covered person would be breaching its statutory duty and depriving the consumer of their statutory right. And that is true regardless of whether the request comes from an "individual or an agent, trustee, or representative acting on behalf of an individual" since all of those meet the statutory definition of "consumer."

[35] *A Financial System That Creates Economic Opportunities, supra* n.28, at 31.

This principle is by no means unique to § 1033. Federal consumer financial protection law is replete with provisions that impose duties on financial institutions triggered by a request or other action by a consumer. For example, under the Truth in Lending Act, a creditor or servicer of a mortgage is required to "send an accurate payoff balance within a reasonable time … after the receipt of a written request for such balance from or on behalf of the borrowers." 15 U.S.C. § 1693g. Under the Electronic Funds Transfer Act, if a consumer disputes a transaction shown on a monthly statement, the financial institution is required to "investigate the alleged error, determine whether an error has occurred, and report or mail the results of such investigation to the consumer." *Id.* § 1693f(a). And, under the Fair Credit Reporting Act, if a consumer notifies a furnisher of information to a consumer reporting agency that the consumer disputes the accuracy of information that the furnisher supplied, the furnisher is required to "conduct an investigation with respect to the disputed information," "report the results of the investigation to the consumer," and, if the information is found to be inaccurate, to "notify each consumer reporting agency to which the person furnished the inaccurate information of that determination." *Id.*. § 1681s-2(E). In each of these cases, it would plainly be a violation of the statute for a party under a statutory duty to fail to discharge that duty–to refuse to supply a payoff statement or to refuse to conduct an investigation of a disputed transaction or a disputed piece of furnished information–unless and until the consumer paid a fee to defray the attendant costs.

In arguing that, as with these other examples, § 1033 precludes data providers from requiring consumers to pay a fee to access their financial data, we do not mean to deny that there may be real costs associated with affording data access. For those financial institutions covered by the Rule that have not yet built an interface through which data can be accessed, there can be one-time, upfront costs in doing so, although institutions that elect to rely on a vendor that already provides them with information technology services (e.g., a core processor or provider of mobile banking functionality) may not be assessed any upfront fees for connecting to the vendor's open banking interface. All covered institutions will incur ongoing costs associated with maintaining the functionality that can respond to consumer data requests; these may take the form of direct costs (for those data providers maintaining their own functionality) or fees charged by a vendor.

The question of who should bear those costs implicates complex policy considerations. As the ANPR suggests, if data providers cannot charge fees for data access, at least the variable costs could, in theory, end up being "shared by every consumer of a covered person, including those who may not wish to exercise their rights under Section 1033."[36] That might suggest that a fairer system would allow for charging user fees to cover these costs, assuming they are actually measurable and material. (When the CFPB sought information from data providers on their costs at least some providers reported that "it was difficult to disaggregate the costs of developer interfaces from their consumer interfaces and other information technology systems." 89 Fed. Reg. at 90961.) On the other hand, checking account customers who do not choose to use online bill pay or remote deposit functionality presumably share in the costs of building and maintaining those systems, just as customers who do not engage in branch banking share in the costs of

[36] Economic theory and empirical research teach that, in general, prices move in relation to changes in marginal costs and not one-time fixed costs. *E.g.,* RBB Economics, Cost Pass Through: theory, measurement, and potential policy implications (Report for the Office of Fair Trading, 2014).

branches. Providing data access could similarly be viewed as one of the bundle of services or features available to checking account customers rather than as a stand-alone feature warranting a-la-carte pricing.

From the perspective of the health of the data sharing ecosystem, the fee issue likewise raises complex, competing considerations. On the one hand, smaller or mid-size players that elect to build their own interface may find it especially challenging to absorb those costs without some remuneration. Yet recent market developments point to the risk that large data providers could use their pricing power to discourage data from being accessed in ways that pose a competitive threat to the data provider, or that large data providers and large aggregators could agree to pricing that put smaller or mid-size data providers and/or aggregators at a competitive disadvantage. And, to the extent data providers were to charge fees for access to their interface, that might stimulate renewed interest among third parties and aggregators in using consumers' log-in credentials to access data notwithstanding the security issues inherent in the sharing of such credentials. Indeed, if fees were left unregulated, one can easily envision a future state in which data providers and aggregators engage in a cat and mouse game, using artificial intelligence or other technological methods, in which data providers seek to protect their fees by detecting and blocking data access through means other than their API while aggregators seek to avoid paying those fees by circumventing such blocks and accessing the data directly.

At a minimum, to prevent anti-competitive behavior and to avoid fees that stimulate new forms of screen scraping, any rule that permitted fees to be assessed should be limited to a "reasonable rate for offsetting the cost of enabling consumers to exercise their rights under Section 1033" as suggested by ANPR Questions 15 and 16. That, however, would open a hornet's nest of challenges for the Bureau.

For example, what constitutes such a "reasonable rate?" Should it cover upfront, fixed costs–including costs that larger financial institutions incurred long before the PFDR Rule takes effect–or only marginal costs? Should it cover the costs of enabling individual consumers to access their data or only the costs of enabling authorized representatives to do so? If the latter, how should reasonable costs be calculated for data providers given that accounting systems likely aggregate costs as part of their information technology budget so that data providers may not be able to quantify their costs in responding to requests from authorized third parties? To what extent should the definition of reasonableness vary based upon the size of the data provider? How should reasonableness be determined for data providers who choose to provide data access on an outsourced basis and who are charged a monthly fee by their vendor? And, should reasonable pricing be calculated on a per account, per connection, or per data call basis? (Pricing on the latter basis would weigh heavily on PFM apps that require current information on the accounts of their users in order to provide timely advice when needed, e.g., to avoid costly overdrafts.)

These questions–both the larger questions as to whether assessing fees for data access is an appropriate means to cover costs as well as the more granular questions that would arise if reasonable fees were permissible–are quintessential policy questions that are best resolved by Congress or, at a minimum, resolved pursuant to a framework established by Congress such as

that contained in the Durbin Amendment with respect to the regulation of debit card interchange fees.[37] As it currently stands, § 1033 does not contain any such construct but rather, as explained above, creates a right of data access for individual consumers and their authorized representatives that is not conditioned on their paying a fee. Accordingly, the Financial Health Network recommends that the CFPB adhere to the conclusion of the PFDR Rule that, absent further congressional action, § 1033 does not allow data providers to charge fees.

III. Does the PFDR Rule Provide Adequate Security Protection for Consumers' Data?

Beginning with the Data Sharing Principles that the Financial Health Network published in 2016,[38] FHN has consistently emphasized the importance of data security within the data sharing ecosystem. That report noted "the use of the OAuth protocol and tokenization for authenticating consumer consent and accounts, as well as the use of APIs for data transfer" but also recognized that "technology will continue to evolve over time." Accordingly the report called for industry collaboration to "define industry-wide standards and protocols for consumer data sharing" and suggested the need for "an independent body to administer and maintain the standards over time in order to fully achieve the principle of Security."[39]

Given this perspective, FHN welcomed the principled-based approach that the PFDR Rule took to the issue of security. Section 1033.421(c) requires an authorized third party to apply to its systems for the collection, use, and retention of covered data an information security program that satisfies the Standards for Safeguarding Customer Information, 16 C.F.R. Part 314, promulgated by the Federal Trade Commission pursuant to the Gramm-Leach-Bliley Act (GLBA).[40] A data provider's obligation to provide a third party with access to data is conditional on the third party providing documentation that it has agreed to abide by this requirement. PFDR Rule §§ 1033.331(b)(iii), 1033.401(b). And, even if the third party provides such documentation, and thus meets the definition of an "authorized third party," a data provider may nonetheless deny access if the third party "does not present any evidence that its information security practices are adequate to safeguard the covered data" or if, based either upon the data provider's vetting of the third party or information otherwise obtained, the data provider becomes aware of a "specific risk of which the data provider is aware, such as a failure of a third party to maintain adequate data security." PFDR Rule §§ 1033.321(b)(1), (d)(1).[41]

FHN likewise welcomed the approach that the PFDR Rule took to screen scraping. Given the security risks posed when consumers share their log-in credentials for their bank accounts, §

---

[37] Dodd-Frank Act, § 1075, 15 U.S.C. § 1693o-2.

[38] CFSI's Consumer Data Sharing Principles, *supra* n.2.

[39] *CFSI's Consumer Data Sharing Principles,* n.2 *supra.*

[40] The FTC Rule applies, in terms, to any financial institution–defined to mean any institution "engaged in any activity…financial in nature or incidental to such financial activity, 12 U.S.C. § 1843(k)--within the FTC's jurisdiction. 16 C.F.R. § 314.1(b). PFDR Rule § 1033.421(b) requires any third party outside of the coverage of the FTC's Safeguard Rule must nonetheless adhere to it with respect to its information security program for covered data.

[41] The cost-benefit analysis accompanying the PFDR Rule estimates that data providers will spend 120 hours vetting each third party seeking data access. 89 FR at 9094.

1033.311(e)(1) expressly requires banks to create an interface that authorized representatives can use to access data without relying on consumers' log-in credentials. The Rule leaves banks free to block third parties from seeking to bypass the bank's interface–and the obligations attendant upon a third party that is authorized to use the interface–so long as the bank "mak[es] the requested data available through a more secure alternative." 89 FR at 90895. And, the Bureau cautioned third parties that "once data providers have enabled the safe, secure, and reliable forms of data access envisioned in this rule…screen scraping attempts by third parties to reach data covered by such arrangements could well be limited by the CFPA's prohibition on unfair, deceptive, or abusive acts or practices." *Id.*

FHN does not believe that the Bureau can do more by rule to achieve data security without becoming overly prescriptive and, potentially, adopting requirements that will not keep pace with technological change. We share the view expressed in the Rule that, within the context of the Rule's principles, "consensus standards will eventually develop around the rule's requirements and the ways that third parties can demonstrate compliance, which will mitigate costs for data providers by putting the onus on third parties to show they are credible and secure." 89 FR at 90964. Indeed, we believe that the Financial Data Exchange (FDX) is well positioned to develop such standards. (Since the Rule was promulgated, FHN has joined the FDX, and a representative of FHN now serves on the FDX Board, having been elected as co-chair of the FDX Non-Commercial Organizations Board Advisory Council.)

We can envision a future state in which there are a set of specific information security standards for third parties seeking to become authorized third parties and a set of certified, independent assessors qualified and empowered to assess a third party's compliance with such standards and certify those that are compliant. Such a system already exists to assure data security through the payment lifecycle, as data moves from consumer to merchant to card issuer,[42] and a similar system is being developed by a newly-formed, industry-led organization focused on risk management standards for fintechs seeking to offer products in partnership with a bank.[43]

The Financial Health Network urges the CFPB to promote the development of such a program by voicing its support and encouragement. As stated above, however, we do not believe the CFPB should seek to be more prescriptive in a revised PFDR Rule with respect to the issue of data security.

IV. Does the PFDR Rule Provide Adequate Protection of Consumer Privacy?

As discussed in Part I, the Rule contains a set of data minimization provisions designed to protect consumer privacy. These include both a restriction of the data that an authorized third party can obtain from a data provider–permitting the third party to obtain only those data elements needed to deliver the product or service the consumer has requested–and a provision prohibiting the third

[42] The PaymentCard Industry Council has developed such standards and trains, tests, and certifies individuals and organizations who in turn can assess and certify compliance with the PCI standards. *See* https://www.pcisecuritystandards.org/standards/

[43] Coalition for Financial Ecosystem Standards, https://thecfes.com/

party from using the data for any other purpose. In addition, the Rule requires authorized third parties to provide a readily accessible means through which a consumer can terminate authorization if the consumer no longer desires to allow access to their data. And, to protect against the possibility of a consumer inadvertently allowing authorization to continue, the Rule establishes a maximum one-year term for each authorization after which the authorization lapses unless expressly renewed by the consumer.

FHN believes that these provisions adequately, indeed robustly, protect consumer privacy. We cannot imagine what more the Bureau could do in this regard. Indeed, in two respects FHN believes that the Rule places limitations on the uses to which covered data can be put that are not necessary to protect consumer privacy and that disserve the goals the CFPB was created to further.

First, the Rule prohibits a third party who has lawfully obtained data with consumers' authorization to deliver a specific product or service to individual consumers from using those data to develop new products or services. This is a necessary consequence of the provision of the Rule that permits an authorized representative to use data only as "reasonably necessary to provide the consumer's requested product or service." § 1033.421(a). That provision leaves no room for using the data for the purposes of developing a new product or service since such product or service, by definition, was not one the consumer requested; in the lexicon of the Rule, product development constitutes a "secondary use" which the Rule disallows.[44] To be sure, the Rule does allow third parties to seek a separate authorization to use data for new product development as a "stand-alone product or service." 89 Fed. Reg. at 90934. But aside from the confusion such a requirement is likely to create among consumers receiving a request for such a second authorization, precluding data lawfully obtained to be used for new product development absent a separate authorization threatens to stifle product innovation. In today's world–and even more so in the world towards which we are rapidly heading–product innovation is to a large extent dependent on the ability of innovators to train models on a representative data set. Limiting the consumer-permissioned data that an authorized representative can use for product development to the data of those consumers who provide a separate authorization can introduce biases in the data that negatively impact the data's reliability and hence utility.

This restriction on the use to which an authorized third party can put lawfully-obtained data does not appear to advance any cognizable privacy interest as "privacy" is generally understood. Permitting such data to be used by the authorized representative for product development purposes would neither expand the data available to the third party nor expose the data to any new entity. Further, analyzing data for product development purposes can be done using an anonymized or pseudoanonymized version of the data–that is, by stripping any personally identifiable information (PII) from each record–so that even the individual researchers employed by the authorized third party to conduct the research could not know the identity of the consumers whose information they were using. Accordingly, if the CFPB proceeds to propose revisions to

[44] *See* 89 FR at 90941 ("uses that are not reasonably necessary to provide the consumer's requested product or service are secondary uses, and are not permitted as part of the third party's authorization to access the consumer's covered data for purposes of providing that product or service")..

the PFDR Rule, the Financial Health Network urges the Bureau to add to § 1033.421(b) an express authorization allowing an authorized representative to use lawfully-obtained data for new product development.

Second, and relatedly, the Rule's prohibition on any "secondary use" precludes an authorized representative from creating an anonymized or pseudoanonymized version of data lawfully obtained and sharing that dataset with outside researchers, such as academics or think tanks, for use in studying consumer behavior, outcomes, and needs. For many research questions in consumer finance, the most relevant data is "covered data" under § 1033, especially transactional data derived from consumers' checking accounts. Authorized third parties serving large customer bases assemble such data in the normal course of business, and some third parties heretofore have been willing to make their data available, in a deidentified form, to bona fide researchers. The PFDR Rule would preclude them from doing so except with respect to those consumers who provide a separate authorization for the use of their (deidentified) data for research.

The impact this limitation would have on researchers' ability to answer important research questions is illustrated by a Request for Information recently issued by the Department of Housing and Urban Development "seek[ing] to better understand how emerging financial products—such as Buy Now, Pay Later (BNPL) loans—may affect FHA-approved mortgagees' ability to fully evaluate a borrower's financial profile and capacity to sustain long-term homeownership." 90 FR 26824 (June 24, 2025). To advance such understanding, the RFI asks for information about, among other things, "the credit and spending profiles of borrowers who frequently use BNPL services," the extent to which BNPL borrowers are "engaging in multiple concurrent BNPL loans (loan stacking)," and the "types of repayment issues…borrowers with BNPL debts experience." *Id.* at 26825. Because BNPL loans generally are not reported to credit bureaus, and because each BNPL lender sees only its own loans and thus has no visibility into loan stacking, the questions that HUD has posed are best answered from transactional data across a representative set of consumers, enabling researchers to identify BNPL borrowers and all their BNPL loans. Indeed, two academic studies of BNPL have been done using precisely such deidentified, transactional data obtained from a data aggregator.[45] Yet under the Rule, these researchers could not have obtained these datasets.

It is precisely because of the value of deidentified, account-level transactional data for research purposes that during the PFDR rulemaking process, over 100 faculty members from roughly 50 colleges and universities in the United States joined in a joint letter to the CFPB describing the value of such data and urging the Bureau to "establish a clear legal protocol for accessing and

[45] deHaan *et al.,* Buy Now, Pay (Pain?) Later (2024); di Maggio *et al.,* Buy now, pay later credit:: User characteristics and effects on spending patterns (2022).

using representative or full samples of de-identified or anonymized transaction data for research purposes."[46] Other research organizations submitted similar comments (as did FHN itself).[47]

To be sure, to the extent deidentified data is shared with researchers, there is a risk that the data could be reidentified, at least where the records in the dataset contain unique attributes that can be matched to other publicly-available datasets containing PII. Were that to occur, consumers' privacy interests would be compromised. But to the extent the Bureau is concerned about the risk of academics or other bona fide researchers seeking to reidentify data, there are a variety of ways in which the CFPB could mitigate the risk, either by limiting deidentified data sharing to bona fide researchers (e.g., academics, think tanks) who commit not to attempt re-identification and/or by requiring that any de-identification or pseudonymization use appropriate tools to reduce the risk that data can be re-identified. Indeed, the academics whose comment letter is referenced above offered a number of suggestions in this regard in an *ex parte* meeting held with Director Chopra and documented in the rulemaking record.[48]

In promulgating the PFDR Rule the CFPB expressly acknowledged "the value of de-identified data for research purposes" and noted that the CFPB "uses de-identified data itself for research and market monitoring." 89 FR at 90942. Indeed, the CFPB stated that "public interest research may present unique considerations not developed in the current rulemaking record" and that the Bureau "will consider whether a follow-on rulemaking would be appropriate to allow for public interest research uses of de-identified data outside of the general standard finalized in this rule" prohibiting any secondary use. *Id.* If the CFPB elects to proceed further towards reopening the PFDR rulemaking, FHN urges the Bureau to use the opportunity to reconsider the prohibition on research using deidentified data.

***

The Financial Health Network again thanks the Bureau for the opportunity to comment on the ANPR. We would welcome the opportunity to discuss our views in person and to provide any assistance that would be helpful.

[46] Comment Letter from Bronson Argyle *et al.,* https://www.regulations.gov/comment/CFPB-2023-0052-0938. The signatories to the letter also included approximately 30 PhD candidates and post-doctoral students, as well as faculty from colleges and universities in Canada, England, Australia, and several other countries.

[47] *E.g.,* Comment Letter from Kelly Cochran on behalf of FinReg Lab, https://www.regulations.gov/comment/CFPB-2023-0052-0971; SaverLife 1033 Comment, https://www.regulations.gov/comment/CFPB-2023-0052-0654

[48] Memorandum from Bronson Argyle, April 18, 2004, https://www.regulations.gov/comment/CFPB-2023-0052-11120