FINANCIAL HEALTH NETWORK

Comment of the Financial Health Network: Required Rulemaking on Personal Financial Data Rights

Docket No, CFPB-2023-0052, RIN 3170-AA78

DECEMBER 29, 2023

The Financial Health Network appreciates this opportunity to comment on the CFPB's Notice of Proposed Rulemaking (NPRM) on "Personal Financial Data Rights" 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 industries, business leaders, policymakers, innovators, and visionaries in a shared mission to improve financial health for all. Because of the significant role that 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 actively engaged with the issues raised by the proposal since 2015. We issued a set of Consumer Data Sharing Principles in 2016,[1] and a set of follow-on recommendations and "call to action for financial service providers and regulators in 2017.[2] Both of these position papers predated the Bureau's own principles. And we have since published several widely-cited research reports on this topic.[3]

Beyond our role as a thought leader in this area, FHN's Financial Solutions Lab 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. Additionally, as a membership organization, FHN includes among its members both "data providers" and "third parties" as defined in the proposal. Moreover, FHN itself would qualify as a third party since, as part of its ongoing research program to better understand and measure financial health, FHN, in collaboration with the USC Understanding America Study, accesses consumer-permissioned data which is linked to responses from FHN's annual Financial Health Pulse® survey to provide more robust insights into the financial health challenges Americans face.[4] All of these perspectives inform the comments below.

---

[1] CFSI's Consumer Data Sharing Principles. At the time these Principles were issued FHN was known as the Center for Financial Services Innovation (CFSI).

[2] Liability, Transparency, and Consumer Control in Data Sharing

[3] *E.g.,* Financial Data: The Consumer Perspective (2021); Consumer Financial Data: Legal and Regulatory Landscape (2020).

[4] For an overview of the Financial Health Pulse®, *see* *https://finhealthnetwork.org/programs/financial-health-pulse/*. The Pulse Points available there illustrate how FHN has used survey and transactional data in our research.

Introduction and Overview

With respect to the consumer financial products the CFPB has elected to cover in its first § 1033 rule, FHN believes that the CFPB's proposal would implement § 1033 in a manner consistent with the important purposes of the statute and with the data sharing principles that FHN has long championed. We thus commend the CFPB for crafting a proposal that would go a long way towards achieving the objectives outlined in the NPRM.

We have two primary recommendations for modifications to the proposal which we set forth in Parts I and II of this Comment. First, we urge the CFPB to expand coverage to include needs-tested EBT accounts and, beyond that, to make clear that once this rulemaking is concluded the CFPB intends to move expeditiously to expand coverage still further. We fear that absent a strong statement along these lines data holders not covered by the final rule will take its limitation as a license to restrict access to data that is plainly within the scope of § 1033, including data that is currently being accessed by data users through secure means to provide products and services that advance consumers' financial stability and well-being.

Second, we urge the CFPB to both narrow and also clarify the scope of the restrictions on secondary use of covered data set forth in the proposal. We are deeply concerned that, if adopted as proposed, these restrictions would severely limit research that can lead to products and product features that advance financial health and advance public understanding of the state of financial health in the United States. We further believe that, absent the changes we propose with respect to secondary use, the rule would have the unintended consequence of entrenching incumbent data holders and of advantaging traditional credit bureau data over transactional data, thereby undermining core purposes of the proposal.
In addition, as set forth in Part III of this comment, we have a myriad of additional recommendations – some technical, some more substantive – designed to clarify certain aspects of the proposal and to address practical challenges we see with other aspects. None of these should detract from our overall view that the CFPB has succeeded in developing a proposed rule that, if adopted, would assure a robust regime of open data sharing with respect to the products the rule covers, while building in flexibility to allow the regime to evolve along with changes in market standards and technology.

FINANCIAL HEALTH NETWORK

I. The CFPB Should Expand Coverage to Include Needs-Tested EBT Products and Should Signal Its Intent to Move Expeditiously to Cover Other Core Consumer Financial Products and Services

Section 1033, in terms, applies to all "covered persons," which is to say to all providers of any "consumer financial product or service" as defined in the Dodd-Frank Act. Understandably, the CFPB has chosen to cover a subset of those products and providers in its initial § 1033 rule. Although in our response to the SBREFA outline we had urged the CFPB to include mortgage, auto, and student loans in its proposed rule, we recognize that those recommendations are no longer in scope for this rulemaking. We also recognize that the products the CFPB has elected to cover are the most commonly held consumer financial products, and that the data covered by the proposal are the data that are most commonly being accessed and used today.

The proposal does invite comment on whether the final rule should include not only accounts as defined in Reg. E but also needs-tested EBT accounts. The answer to that question, in our view, is an emphatic yes.

Needs-tested EBT accounts do not constitute "accounts" under Reg. E because of a carve out in the Electronic Fund Transfer Act that is wholly unrelated to the purposes underlying § 1033.[5] But from the perspective of an open data sharing regime, there are compelling reasons to include these accounts.

Abundant research demonstrates that recipients of SNAP benefits – a primary source of needs-tested EBT benefits – find it challenging to make their monthly allotments last for a full thirty days.[6] If data with respect to recipients' accounts were available through the § 1033 rule, third parties could use these data to provide personal financial management services including, for example, budgeting tools and tools to help recipients drive down the cost of the food they purchase. Further, affording access to information on needs-tested EBT accounts will allow third parties to

[5] 15 U.S.C. § 1693b(d)(2).

[6] *E.g.,* U.S. Dep't of Agriculture, Benefit Reduction Patterns in the Supplemental Nutrition Assistance Program (2011); Marchesi, The Impact of the SNAP Distribution Cycle on Student Non-Cognitive Outcomes (2019).

aggregate these data with data regarding other accounts recipients may have, and thus obtain a more complete picture of the recipients' financial situation and find ways to help them better manage their financial lives. These are precisely the type of services that consumers with Reg. E accounts will be able to enjoy under the proposed rule. Recipients of needs-tested benefits – who are among the most vulnerable individuals in our society – should not be deprived of the same opportunities.

Beyond these potential benefits of covering needs-tested EBT accounts, it is an unfortunate reality that the payment processors for these benefits provide consumer interfaces that are fundamentally flawed both in terms of the data they provide and the speed with which they provide it. Because these processors do not compete for the benefit recipients' business, they have little incentive to improve these interfaces. Covering these accounts under § 1033 with mandatory data requirements and performance standards for a developer interface would bring a form of competition to this market and improve the service that recipients receive from consumer interfaces. This is yet an added reason for providing for such coverage in the final rule.

A rule that covers Reg. E accounts, needs-tested EBT accounts, and credit cards as defined in Reg. Z would mark a strong beginning to implementing § 1033. But such a rule would be only a beginning. To realize the full potential of § 1033 as a building block for advancing consumers' financial health, it is vitally important that, in subsequent rulemakings, the definition of "covered consumer financial product or service" be expanded to cover a range of other products or services.

For example, for a consumer who authorizes a third party to access the transactional data that will be available with respect to checking accounts under the proposed rule, it generally will be possible for the third party to identify payments the consumer is making on various credit products, including mortgages, auto loans, student loans, and personal loans. But absent information about the features of those loans – at a minimum, the interest rate, the outstanding balance, and the remaining term – it will not be feasible for the third party to advise the consumer as to whether to seek out less-costly alternatives (for example, by refinancing a mortgage or consolidating credit card debt) or how to optimize their payments on existing loans. Yet one of the goals animating the enactment of § 1033 was precisely to enable data to be used for these purposes.[7] To achieve that goal – a goal closely connected with the overall aim of advancing consumers' financial health – a follow-on rulemaking should address these other credit products.

[7] *See generally,* R. Thaler & C. Sunstein, *Nudge* at 144-50 (2021).

Similarly, it has become increasingly clear that access to payroll data maintained by payroll processors can play a vital role in realizing the benefits of open data. From a cash flow underwriting perspective, although transactional data from checking accounts provides insights into a consumer's net income for consumers who have opted for direct deposit, payroll data provides the most authoritative and up-to-date evidence of a consumer's wage rate, hours worked, and both gross and net income and does so for all consumers paid through a payroll processor; such data thus can buttress the development of cash flow underwriting. Further, data aggregators such as Pinwheel, Atomic, and Argyle that specialize in accessing payroll data have built the capacity to enable consumers to immediately redirect their direct deposit from their current bank to a new one, thereby eliminating one of the primary impediments to switching banks and facilitating a more competitive banking environment, as the Bureau is seeking to do. Accordingly, a follow-on rulemaking should expand the definition of covered consumer financial products and services to cover payroll processing as well as mortgages, auto loans, student loans and other installment loans covered by Reg. Z.[8]

There is a material risk that, once this rulemaking is concluded, data holders in markets that are left untouched by the rule will assume that § 1033 will not reach them at least for the foreseeable future, especially in light of the length of time that will have elapsed between the enactment of Dodd-Frank and the promulgation of this rule. Were these data holders to reach that conclusion, entities that today make data available with respect to products that fall outside of the proposed rule – e.g., pursuant to bilateral agreements they have entered and APIs they have created – may elect to withdraw those data from their APIs or may make those data available only through preferred APIs that charge an access fee. Efforts to negotiate new bilateral agreements to access data for non-covered products may become more challenging as the data holders may assume that they have all of the leverage in such negotiations. The end result could be either a reduction in data flow or an increase in the use of less safe methods to access data, such as screen scraping using a consumer's log-in credentials and could issue an Advanced Notice of Proposed Rulemaking concurrently with the final rule identifying products of interest for a follow-on rulemaking.

[8] Payroll processing can easily be viewed as "providing payments or other financial data processing products or services to a consumer by any technological means," and thus as a "financial product or service" under § 1002(15)(vii) of the Dodd-Frank Act, 12 U.S.C. § 5481(15)(vii). Payroll processing also could be defined as an "other financial product or service" under § 5481(15)(xi).

To mitigate these risks, we urge the Bureau, as part of its final rule, to send a direct message that (a) § 1033 applies to all "covered persons" and not just those covered by this initial rule and (b) the Bureau intends to move expeditiously to conduct a follow-on rulemaking. Indeed, the Bureau could list such a rulemaking in its Spring 2024 Regulatory Agenda to make its intent even clearer.

II. The Bureau Should Clarify and Narrow the Scope of the Restrictions on Third Parties' Secondary Use of Covered Data (§1033.421(c))

Under proposed §1033.401, a third party can access covered data only if a consumer has authorized it to do so after receiving a disclosure describing, among other things, the product or service that the consumer has requested the third party to provide and the categories of covered data that will be accessed. Further, under proposed §1033.421,the third party must commit to "limit its collection … of covered data to what is reasonably necessary to provide the consumer's requested product or service." As discussed further below, we support both of these requirements as integral to two of the principles which we have long espoused: consent and minimization.

In addition to these requirements, proposed §1033.421(c) also requires third parties to restrict their use of data that has been collected pursuant to the limitations set forth above to "what is reasonably necessary to provide the consumer's requested product or service." The scope of this limitation is, in our view, in certain respects uncertain and in other respects overbroad in that it will interfere with activities that are vitally important to advancing financial health and assuring, in the words of the Dodd-Frank Act that consumers have "access to consumers financial products and services" from markets that are "fair, transparent, and competitive." Moreover, the proposed limitation is not necessary to further any cognizable privacy interest insofar as it applies either to a third party's own use of data that the consumer has authorized that party to obtain or to the sharing of a de-identified or pseudonymized version of such data so long as adequate steps have been taken to prevent re-identification.

We thus suggest four modifications to the proposal.[9]

[9] The discussion that follows uses terminology, and a modified version of a topology, suggested by FinRegLab in its Comment on Outline of proposals and Alternatives Under Consideration for Required Rulemaking on Personal Financial Data Rights at 8 (Jan. 25, 2023).

First, the Bureau should clarify the "reasonably necessary" standard to expressly allow third parties to engage in "supplemental primary uses." To a very large extent, the data that will be available under the rule is useful in delivering a product or service to an individual consumer because it enables a third party to make a prediction about that consumer based upon prior learnings from data previously accumulated. In the cash flow underwriting context, for example, lenders use transactional data to make predictions about whether a given consumer has the ability to repay a contemplated extension of credit. In the personal financial management context, providers use such data to make predictions about whether, e.g., a given consumer can afford to move money into a savings vehicle at a given moment in time or, at the opposite end of the spectrum, whether a given consumer is about to run short and needs a cash infusion to avoid overdrafting.

In order to be able to continue to deliver such services effectively and efficiently, the third party providers need to be able to continue to learn from their experience, thereby improving the accuracy of their algorithms and predictions. In some instances, such learning can redound to the benefit of the very consumers whose data is being used and thus would seem to fit comfortably within the "reasonably necessary to provide the consumer's requested product or service" framework. But in other instances, the learning will benefit only future customers or would-be-customers as would be true, for example, of learning that refines a cash flow underwriting model used to determine to whom to extend credit going forward. Yet such learning is no less important than learning that improves algorithms used to deliver ongoing services to existing customers. Thus, we urge the Bureau to clarify that improving or assessing outcomes with respect to a product or service that the consumer has requested is "reasonably necessary to provide the consumer's requested product or service."

Second, the Bureau should modify the secondary use limitation to permit third parties to use covered data that they have lawfully obtained for the purpose of conducting research to support the development and testing of new products or product features. Just as many of the existing use cases for covered data depend on the application of algorithms or other models built on historical data, so, too, will the ability of third parties to innovate further depend on their ability to use data to test the feasibility of ideas they may dream up. Such product development, by definition, is not "reasonably necessary to provide the consumer's requested product or service." But if such use is prohibited, as the proposal as written almost surely would do, the offerings of third parties would be frozen in place. That would be an unfortunate result, to say the least, especially given the CFPB's

mandate of "ensuring that … markets for consumer financial products and services operate transparently and efficiently to facilitate access and innovation."[10]

A real-world illustration may help make this more concrete. Petal Card Inc., which FHN was proud to help incubate as part of its Financial Solutions Lab, was founded to provide credit to the credit invisible and underserved. It has pioneered the use of cash flow underwriting for these purposes. Over time, Petal came to realize that there was both a market and consumer need, as well as a business opportunity, to turn its learnings into analytical tools that other lenders could use to do their own cash flow underwriting. Accordingly, Petal incubated the now-independent Prism Data Technologies, Inc. using de-identified consumer-permissioned data from Peta's credit card customers coupled with de-identified data that others had similarly acquired and shared with it. Today, Prism offers a set of tools, including its CashScore,™ that can be used by lenders to analyze transaction data for credit risk assessment purposes and can supplement or supplant traditional credit scores. None of this would have been possible under the strictures of the proposed rule.

Third, the Bureau should modify the secondary use limitation to permit a de-identified or pseudonymized version of lawfully-obtained covered data to be used for "secondary public use" – that is, for research by the authorized third party or by outside researchers who commit to using the data only for bona fide research purposes. Covered data is valuable, of course, not only to inform research towards potentially profit-making activities, such as product development and testing, but also to support research that will further understanding of consumer behavior, outcomes, and needs in much the same way that the CFPB currently uses de-identified credit data in its Consumer Credit Panel and de-identified transactional data (aggregated at the monthly account level) in its Credit Card Database to support invaluable research. Such "secondary public use" also should be permitted under the rule.

The JPMorgan Chase Institute has pioneered the use of transactional data – albeit data obtained from affiliates within the JPMC family – for research purposes and demonstrated how valuable such data can be. Studies of cash flow underwriting--including, for example, FinRegLab's groundbreaking study[11] that the NPRM itself cites as establishing the benefits of such underwriting – could not have been conducted under the proposed rule since it was predicated on an analysis of what would be "covered data" under the proposal. Nor would the research on buy now, pay later products that was presented at the CFPB's 2022 Research Conference have been possible under the proposal rule

[10] Dodd-Frank Act § 1021(b)(5), 12 U.S.C. § 5511(b)(5).

[11] FinReg Lab, *Use of Cash-Flow Data in Underwriting Credit: Empirical Research Findings* (2019).

since both of the papers presenting that research used transactional data from third parties.[12] And, to cite one more example, SaverLife, a non-profit that FHN is proud to have helped incubate as part of its Financial Solutions Lab, explains on its website that one of its purposes is to "publish and share groundbreaking reports and publications that leverage the financial data" that its members "entrust us with"; the website has a long and impressive list of research reports it has prepared or that its research partners prepared utilizing de-identified data obtained from SaverLife.

Of course, to the extent that third parties share de-identified or pseudonymized covered data with outside researchers, there is a risk that the data could be reidentified, thereby compromising consumers' privacy interests. The CFPB could, however, mitigate that risk by permitting such sharing only to bona fide researchers who commit not to attempt re-identification, along the lines of a trusted researcher program. Additionally, if the CFPB deemed it appropriate, it also could require that any de-identification or pseudonymization use appropriate tools to reduce the risk that data can be re-identified while leaving room for transactional data to be linked to other datasets through techniques that do not require reidentification (perhaps looking to a "qualified industry standard" as an indicia of compliance). In all events, the Bureau should leave room for "secondary public uses" in the final rule.

Fourth and finally, the CFPB should permit third parties to use data that they have lawfully obtained with a consumer's consent, to offer additional products or product features that may be useful for the consumer. Proposed § 1033.421(a)(2)(i) and (ii) expressly prohibit third parties from using covered data for "targeted advertising" or "cross-selling of other products or services." Insofar as it applies to third parties offering personal financial management services (PFMS), the scope of that prohibition is somewhat unclear as it is uncertain when a recommendation of a particular product or service is the very thing that the consumer has sought from the PFMS provider and when a recommendation crosses the line into cross-selling. For example, it seems clear that a third party offering a PFMS product could recommend to a given consumer that the consumer consolidate identified, high-cost debt into a personal installment loan. But if the third party went further and recommended a specific loan, or provided the consumer with a set of options to explore, would the third party cross the line into impermissible cross-selling? If so, the rule would have the paradoxical effect of permitting third parties to provide generalized advice and forcing consumers to figure out how to implement the advice while disabling third parties from providing much more concrete and actionable assistance.

[12] deHaan *et al.*, *Buy Now Pay (Pain) Later*; Di Maggio *et al.*, *Buy Now, Pay Later Credit: User Characteristics and Effects of Spending Patterns.*

In other cases, the application of the proposed prohibition on target advertising and cross-selling is clear and, in our view, unduly restrictive. Many fintechs offer consumers an entry-level product at no cost or for a minimal price and then offer at least some of their consumers the opportunity to purchase a richer set of benefits for a higher fee. Under the proposed rule, third parties would be free to make such offers to their customers on an indiscriminate basis. If, however, a third party sought to use "covered data" to offer such additional features to only those consumers whom the data shows would most benefit from the feature, the third party would be guilty of violating the rule. Thus, for example, a third party could offer a credit building feature to all of its customers but not to those customers who, based on the covered data available to the third party, would seem most likely to benefit from the service. Similarly, a third party could offer an overdraft protection feature to every customer but not to those whom the covered data indicates most often incur avoidable overdrafts. This would turn the purpose of the data sharing regime contemplated by the rule on its head.

We recognize, of course, that cross-selling creates a risk that consumers will be sold products or services of limited (or even no) utility to them. But that risk exists regardless of whether covered data is used to determine to whom to offer the product; indeed, if anything, the risk is greater if cross-marketing occurs indiscriminately rather than on a targeted basis to those whom data indicates are most likely to benefit from the product being cross-sold. And, in any event, the solution to problematic marketing is the use of the Bureau's UDAAP authority – as the Bureau demonstrated in the credit card add-on cases – and not a blanket prohibition on the use of covered data by an authorized third party for cross-marketing purposes.
The foregoing explains why the modifications in the proposal discussed above are needed to further the consumer protective purposes of § 1033. There is one additional point that needs to be made. The secondary use limitations contained in the proposal of necessity apply only to third parties and only with respect to "covered data" obtained on behalf of a consumer. The inevitable effect of those limitations, if they were to be finalized, would be to create an unlevel playing field as between traditional credit data and "covered data" and between data providers and third parties.

Consumer reporting agencies are, of course, free to provide a de-identified or pseudonymized version of data that they collect to third parties. That is the method that has enabled the CFPB, the Federal Reserve Bank of New York, and various research organizations such as the Urban Institute and the California Policy Lab to procure consumer credit panels. It is also the method that modelers such as FICO or VantageScore use to build and refine their credit scoring algorithms. Yet under the proposed rule it would not be possible to obtain de-identified or pseudonymized transactional data

for these purposes. That would effectively create a competitive advantage for traditional consumer reporting agencies.

Similarly, the proposal would advantage incumbent financial institutions over challengers seeking to disrupt their hold on the market. The reality is that in today's world – and the world of the foreseeable future – the bulk of covered data is held by large banks. Those banks would be entirely free under the proposed rule to use their transactional data to refine existing products, develop new products, and to target market and cross-sell new and existing products to their customers. They would be free to share or sell de-identified data – that is, data that does not include "nonpublic personal information" as defined in the Gramm-Leach-Bliley Act (GLBA) – with any other person or entity.[13] And, they even would be free to share or sell data that is personally identifiable with any other person or entity for whatever purpose that person or entity deemed appropriate (including cross-marketing) so long as such sharing was provided for in the bank's privacy policy and so long as the bank did not share data with respect to those who opted-out from sharing pursuant to the GLBA. That would almost surely create a competitive advantage for large banks vis a vis third parties who access covered data pursuant to the rule, thereby further entrenching the large incumbent players.

To be clear, we do not mean to suggest that third parties who obtain covered data as the representative of consumers should have the same degrees of freedom to use such data as the GLBA provides financial institutions writ large. We agree, for example, that consumers should not be required to opt out to prevent their data from being sold to third parties at least if the data being sold contains personally identifiable information even though data providers are free to engage in such sales. Our point is simply that, in crafting restrictions on secondary uses, the Bureau should be mindful of potential unintended consequences as well as the potential benefits of certain types of uses.

In response to the questions posed in the Notice of Proposed Rulemaking (NPRM), we do not believe that any of the secondary uses described above should be conditioned on consumer's opt-in consent. Behavioral scientists have convincingly demonstrated that increasing the number of choices presented to consumers can lead to "choice overload" and result in decision paralysis such that consumers throw up their hands and elect not to proceed with a transaction.[14] Financial institutions have learned this lesson well and strive to create streamlined application processes with minimal choices for consumers.

[13] 15 U.S.C. § 6809(4); 12 C.F.R. § 1016.3(p1)(1), 1016.3(q)(2)(ii)(A)–(B).

[14] *E.g.,* Chernev *et al.,* *Choice Overload: A Conceptual Review and Meta Analysis* (2015); The Decision Lab, *Choice Overload*.

In the current context, before starting the process of authorizing data access, consumers may face a choice between alternative products or services offered by a third party. They then may face a choice as to the accounts to which they will authorize data access. If, on top of that, consumers were also asked to decide whether to authorize the third party to use their data for product development purposes and were also asked to decide whether to authorize the third party to use their data for secondary public uses and were also asked to decide whether to permit the third party to share de-identified data for secondary public uses and were also asked to decide whether to permit the third party to use their data for cross-marketing, the predictable result would be a much higher abandonment rate and fewer authorizations for any data sharing.

Additionally, if data could be shared only on an opt-in basis for research purposes, the resulting dataset might not be representative of the underlying population, as those who read through the choices and opted in might be systematically different from those who did not do so. This would introduce a selection bias that could compromise the validity of any resulting research. It is our understanding that it is at least in part for this reason that the CFPB has itself consistently resisted calls to limit its datasets to those who opt in to sharing data with the Bureau.

If allowing the secondary uses we have recommended implicated countervailing privacy interests at stake, those would have to be balanced against the risk of choice overload in deciding whether to limit such uses to those who opt in. But, as noted above, we do not believe that the secondary uses we recommend raise cognizable privacy interests. Given the downsides of requiring opt-in as discussed above, we believe the better approach would be to add to the authorization disclosure required under proposed § 1033.411(a)(3) a brief explanation of the ways in which data that identifies the consumer can be used by the third party accessing the data, and to add to § 1033.411(a) a further requirement that the disclosure state that the data can be used for research purposes if stripped of any personal identifiable information.

III. Suggested Clarifications and Refinements to the Proposed Rule

As noted at the outset, in addition to the substantial issues just discussed, there are several other respects in which we believe clarification or refinement of the proposal is warranted to better

achieve the objectives of § 1033 and of the Consumer Financial Protection Act as a whole. We present these recommendations through the lens of the five data sharing principles that FHN put forward in its 2016 white paper: availability, reliability, security, consent, and minimization.

A. Availability (§§ 1033.211, .301(a),(c), .311)

The first requisite for a robust data sharing regime is that "Consumers have the ability to view their financial information within the trusted and secure third-party application of their choice."[15] Towards that end, the proposal defines the data elements that must be made available (§ 1033.211), requires data providers to maintain a consumer interface and a developer interface (§ 1033.301(a)), and sets forth requirements for developer interfaces (§ 1033.311), including requiring that data be made available in a standardized format and that the interface's performance is commercially reasonable, and a prohibition on "unreasonably restricting the frequency with which [the interface] receives and responds to requests for covered data from an authorized third party." These are all necessary elements to ensure availability and thus we support these elements of the proposal.

Proposed §1033.301(c) further provides that a data provider must not impose any fees or charges on a consumer or an authorized party in connection with either establishing or maintaining the interfaces or processing requests for data. The proposal buttresses this provision with prohibitions on discrimination between consumers or third parties which we understand to include a prohibition on favoring those who agree to pay a fee over those obtaining a free service. These provisions are equally important to ensure availability as contemplated by § 1033 and we thus support them as well. Indeed, it is difficult to imagine how § 1033 could be interpreted to grant consumers the right to access data and then allow data providers to condition consumers' exercise of that right on a payment. Although there are some consumer financial protection laws that authorize charging fees for the exercise of a right – for example, for consumers who request a consumer report more than once per year[16]--§ 1033 is not one of those laws.

[15] *CFI's Consumer Data Sharing Principles, supra* n.1, at 4.

[16] In a similar vein, the Bureau may want to adjust certain of the other data elements under the definition of "covered data" to account for industry practices. For example, the proposal requires that data providers make data available with respect to "rewards credits." For co-branded credit card programs, however, rewards are earned in the currency of the co-brand partner (e.g., frequent flier miles) and tracked by the co-brand partner. (Indeed, it may not even be feasible for the data provider to make available the reward program terms.) Similarly, boilerplate arbitration agreements often have a carve out for service members but data providers may not have information in their system of record indicating whether a given customer is in the military at a given moment in time.

While we thus support the provisions discussed above, we offer the following recommendations that we believe will strengthen the availability of data under the rule:

Definition of covered data (§ 1033.211):

We suggest two modifications to the proposed definition.

First, the Bureau should add as a required data element information regarding the name, address, and account number of any entity to which the consumer has authorized the data provider to direct payments. One of the impediments to account switching is the time and effort required to reconstruct push and pull payments with a new financial institution. With respect to push payments, that burden can be relieved by facilitating the transfer of payee information to a new financial institution of the consumer's choosing. We note that because a consumer's account numbers at payees such as utilities or telecoms can only be used to push payments and not to pull money, requiring access to such account numbers would not create security risks.

Second, we recommend that data providers be required to make available historical transaction information through the developer interface for at least as long a period as such data is available through the consumer interface, with a minimum requirement of 24 months. As currently drafted, the proposal creates a safe harbor for data providers who make 24 months of data available. The 24-month period is consistent with current industry standards for online banking portals, which in turn reflect industry norms with respect to the length of time before historical data is archived. We agree with the Bureau's decision to defer to these standard practices. However, practices can change and, given the potential value of historical information, especially in assessing a consumer's financial stability as part of cash flow underwriting, we see no reason to freeze the status quo in place with respect to the length of time for which data must be provided.

Access cap prohibition (§ 1033.311(c)(2)).

The proposal states that a data provider cannot "unreasonably restrict the frequency with which it receives and responds to requests for covered data," and provides that adherence to a qualified industry standard constitutes an indicia that restrictions on access are reasonable. This is a critical issue to assure data availability, as today data providers operating under bilateral agreements do impose caps on the frequency with which an aggregator can call data or the volume of data that can be called within a given time period. This can frustrate the intent of consumers who have, for example, authorized data access to verify in real time transactions in which they seek to engage, or

who have authorized a personal financial management app to monitor their transaction accounts and alert them of impending cash shortfalls.

The section-by-section discussion of this provision addresses this concern by stating that "the CFPB "does not intend that [this provision] would allow a data provider to impose restrictions that would override a consumer's authorization, including the frequency with which an authorized third party requests data." We urge the CFPB to build this limitation into the regulatory text itself by adding after the prohibition on "unreasonably restrict[ing] the frequency with which [a data provider] receives and responds to requests for covered data" the phrase "including restrictions that would override a consumer's authorization."

The section-by-section goes on to state that, "the proposed provision would allow restrictions only if they reasonably target a limited set of circumstances in which a third party requests information in a manner that poses an unreasonable burden on the data provider's developer interface and impacts the interface's availability to other authorized third party requests." But whether a third party's requests will impact an interface's availability depends, at least in part, on the capacity of the interface and the CFPB surely does not intend to allow data providers to build developer interfaces with constricted capacity and then rely on that capacity limitation to refuse data calls. Further, it is unclear what the Bureau means by the "circumstances in which a third party requests information," especially in light of the fact that a "third party" could be anyone from an aggregator serving vast numbers of end users to a single app serving a small customer base. We thus urge the Bureau to clarify this discussion and, at a minimum, to make clear that a data provider cannot impose an access cap if the need to do so is the result of its own failure to create a developer interface with sufficient capacity to handle a reasonably expected, normal traffic load.

B. Reliability/Accuracy (§§ 103.351(c)(1),(2), .421(d))

For consumers' right to obtain data to be meaningful, consumers "need to be able to trust that their data are up-to-date, accurate and complete."[17] the data that is available to them must be accurate. This means, in the first instance, that the data that is accessible through the developer interface must mirror the data that is in the data provider's system of record. The proposal would require data providers to maintain policies and procedures "reasonably designed to ensure that covered data are accurately made available through the data provider's developer interface" (§ 1033.351(c)(1)). We support the inclusion of this requirement and agree with the Bureau's

[17] *CFSI's Consumer Data Sharing Principles, supra* n.1, at 5.

preliminary determination "that a data provider's policies and procedures should be designed to ensure that the covered data that a data provider makes available through the developer interface matches the information that it possesses in its systems."

Proposed § 1033.351(c)(2) goes on to specify certain elements that a data provider "must consider" in "developing its policies and procedures regarding accuracy." We recommend that the Bureau add "accuracy testing" to this list so that data providers, in adopting accuracy policies and procedures, will regularly test whether data in the developer interface in fact matches data in the system of record. We further recommend that, in addition to requiring data providers to publish information on the performance of their developed interfaces as provided for in § 1033.331(d), the rule also mandate that data providers periodically publish information on the results of their accuracy testing.

Data that is accurately loaded into a developer interface can be corrupted in the process of transmission to a third party end user. This is largely because of the role that data intermediaries play in the data ecosystem. We use the term "data intermediary" to refer both to aggregators and also to other third parties, such as Prism Data or Nova Credit – another alumnus of FHN's Financial Solutions Lab – which are in the business of cleaning, analyzing, categorizing, summarizing, normalizing or otherwise manipulating the data obtained from a developer interface to make those data more usable or intelligible to their data user clients.
Proposed § 1033.421(d) addresses this issue by requiring that a "third party will establish and maintain written policies and procedures that are reasonably designed to ensure that covered data are accurately received from a data provider and accurately provided to another third party, if applicable." Although we support the general thrust of this provision, we suggest that for the sake of clarity the Bureau may want to more clearly distinguish between the obligations of third parties who are purely data recipients – and who simply need to be able to accept data in the format in which it is provided so that nothing gets lost or mistranslated in transmission – and the obligations of third parties who function as data intermediaries.

Beyond this, we note that although we agree with the Bureau that data intermediaries who provide data to creditors generally constitute "consumer reporting agencies" within the meaning of the Fair Credit Reporting Act (FCRA), application of the FCRA to data intermediaries as defined above will pose a number of novel questions. For example:

- Given that data intermediaries obtain data on behalf of a third party (who in turn is acting as the representative of consumers) and these intermediaries may not be authorized to retain

the data they obtain for a given third party or to combine those data with data obtained with respect to a single consumer for multiple (authorized) third parties, what obligations do data intermediaries have with respect to providing consumer reports to consumers at their request?[18]

- Given that data intermediaries do not obtain data from "furnishers" as the term has traditionally been understood but rather obtain data by pulling from a developer interface that data providers are obligated to create, what are the obligations of a data intermediary in the event of a consumer dispute regarding the accuracy of the data pulled from the data provider? For example, are data intermediaries obligated to forward the dispute to the data provider and/or to delete disputed information that cannot be verified?[19] Indeed, what would it mean to obligate data intermediaries to "delete" data given the limits on what data they can retain?
- More generally, given that data intermediaries do not determine whether to onboard a particular data provider and do not (or may not) have the option to return files deemed to raise accuracy issues at least to the same extent as a consumer reporting agency can with traditional furnishers, what are the "reasonable steps to assure maximum possible accuracy" that data intermediaries are expected to follow?[20]

We do not believe that the Bureau needs to, or even necessarily can, resolve these issues in this § 1033 rulemaking. The Bureau may, however, want to acknowledge some of these complexities in promulgating the final rule and announce its intent to address them in the context of the Bureau's forthcoming FCRA rulemaking.

C. Consent (§ 103.331(b)(1),(2), .401, .411, .421(b)(2),(3),(h))

The third core data sharing principle that FHN has espoused is that "consumers provide explicit consent for access to and use of their data" and that consumers "can easily view, modify and revoke consent for data sharing."[21] The proposal addresses this principle through provisions addressed to initial authorization, termination and reauthorization, and the role of data providers in the authorization process. We address these in turn:

[18] *Cf.* 15 U.S.C. § 1681j.
[19] *Cf. id.* § 1681i.
[20] *Id.* § 1681e(b).
[21] *CFSI's Consumer Data Sharing Principles, supra* n.1, at 4.

Initial Authorization: Under the proposal, third parties who seek to become "authorized" to access data must provide the consumer from whom authorization is sought an "authorization disclosure" and obtain "express informed consent" (§ 1033.401(a),(c)). The proposal further requires that the disclosure be "clear, conspicuous, and segregated from other material," that it identify the third party, the data provider from whom data is to be obtained, the product or service that the consumer has requested, and the categories of covered data that will be accessed (§ 1033.411(a)). FHN supports these requirements.

In response to questions the Bureau asked in the NPRM, although we recognize the risk that prolix disclosures could result in information overload and increase the likelihood that consumers will scroll through the disclosure, we are nonetheless skeptical that it would be feasible to establish a maximum word count for the required disclosure given that a single authorization could potentially cover multiple products or services, multiple data providers, and even multiple third parties (e.g. an aggregator, an intermediary that analyzes the data, and the end user). To reduce the risk of large amounts of legalese, the Bureau may want to clarify that the required disclosure need not list the various obligations to which the third party is committing under § 1033421; indeed the Bureau may want to offer a model clause that can be used to certify agreement to those obligations.[22] We would, however, support a reasonable maximum reading level requirement as well as formatting requirements.

Termination and Reauthorization:

With respect to termination of authorization, the proposal requires third parties to provide consumers with a mechanism to revoke their authorization that "is as easy to access and operate as the initial authorization" (§ 1033..421(h)). The proposal further establishes a maximum authorization term of one year and allows third parties to seek reauthorization in a "reasonable manner: (§ 1033.421(b)(2),(3)). The failure of a consumer to do so would cause the authorization to collect or retain data to end just as if the consumer had expressly revoked consent (§ 1033.411(b)(4)). We are generally supportive of these provisions but recommend two modifications:

[22] Under 12 U.S.C. § 5532(b), if the Bureau were to adopt a "model form," it would be required first to conduct consumer testing. However, the Bureau may not be so limited in issuing model clauses that fall short of constituting a model form. Alternatively, the Bureau could choose to test the language of a model clause on a limited basis before finalizing the rule as it did, for example, with respect to mortgage servicing early intervention model clauses. *See* 78 FR 10696, 10703-10704 (Feb. 14, 2013).

First, we do not believe that, in seeking reauthorization when the one-year initial authorization expires, third parties should be required to provide the full disclosure required initially but rather should be permitted to use a more streamlined procedure in which consumers are asked to consent in writing to permit the third party to continue accessing the data it has been accessing to deliver the product or service it has been delivering. This may be contemplated by the proposed regulatory text allowing third parties to obtain reauthorization in a "reasonable manner." However, the section-by-section analysis accompanying this provision states that "to collect covered data beyond the one-year maximum period, the third party will obtain a new authorization from the consumer pursuant to proposed § 1033.401(a)." The quoted cross-reference implies that the renewed authorization requires the same level of formality as the initial authorization, including a new disclosure with all of the content required for the initial authorization. We believe this is overkill. Of course, if the authorization lapses and the consumer subsequently seeks to restart it, the full authorization process should be required.

Second, with respect to consumers who are actively using the product or service during the month preceding the expiration of authorization, we recommend that, in lieu of requiring third parties to obtain a new authorization, third parties be permitted to provide an opt-out option to such consumers along with a disclosure that data access will continue as previously authorized unless the consumer elects to opt out within x days. We believe that in this limited context, opt-out is preferable to opt-in to avoid a disruption of a service that a consumer is taking advantage of – a disruption that easily could occur if the consumer were to be inattentive to a renewal notice that required the consumer to affirmatively reauthorize the continued collection of data.

The Role of Data Providers in the Consent Process:

Under the proposal, subject to the security rules discussed below, a data provider must make covered data available to a third party who has provided information sufficient to authenticate the consumer's identity and the third party's identity and to "confirm the third party has followed the [required] authorization procedures" (§ 1033.331(b)(1)). Additionally, the proposal allows a data provider "to confirm the scope of a third party's authorization by asking the consumer to confirm (i) The account(s) to which the third party is seeking access and (ii) The categories of covered data the third party is requesting to access" (§ 1033.331(b)(2)). And, the proposal expressly permits data providers to "mak[e] available to consumers a reasonable method to revoke any third party's authorization to access all of the consumer's covered data and further provides that "To be

reasonable, the revocation method must, at a minimum, be unlikely to interfere with, prevent or materially discourage consumer's access to or use of the data" (§ 1033.331(e)).

We are generally supportive of these provisions with two qualifications.

First, in the section-by-section analysis accompanying proposed § 1033.331(b)(2), the Bureau states that it has "preliminarily determined that data providers should confirm the third party's authorization with the consumer." Although we agree that data providers should be permitted to obtain confirmation, we do not believe this should be viewed as a best practice or expectation of data providers. A data provider may find, for example, that consumers routinely confirm authorization and that the confirmation process is not adding any value either in general or with respect to particular third parties who have proven to be reliable transmitters of authorizations. Thus, we urge the Bureau to state only that this is permissible rather than expected.

Second, we urge the Bureau to add to the provision authorizing data holders to confirm a consumer's authorization a limitation that the data provider is permitted to do so "in a reasonable manner," paralleling the limitation in proposed § 1033.331(e) with respect to revocation procedures created by a data provider. Requiring data holders who choose to confirm authorization to do so in a reasonable manner would preclude data providers – whom, as the Bureau has recognized, may have incentives to discourage data access – from seeking to disrupt the authorization process (e.g. by offering a competing product or service as part of the process of confirming an authorization) or to dissuade the consumer from proceeding. The Bureau could point to compliance with a qualified industry standard as an indicia of the reasonableness of a data holder's confirmation process.
In response to the Bureau's question, we do not believe the Bureau should limit the authorization for data providers to confirm a consumer's authorization to cases in which doing so is "reasonably necessary" as that would open up a Pandora's box of questions as to when confirmation is "reasonably necessary." Rather, as discussed above, we urge the Bureau to disclaim any view of whether or when confirmation is necessary or even appropriate and instead simply create the permission for data providers to confirm authorization so long as they do so in a reasonable manner.

D. Security (§§ 1033.211(c), .311(d). .321, .421(e))

The fourth principle FHN has championed is that "All entities follow applicable laws and industry best practices with regard to data privacy and security."[23] The proposal addresses the need for security in several different ways.

Security of Developer Interfaces: With respect to developer interfaces, the proposal requires data providers to maintain an information security program that meets the applicable rules issued pursuant to the GLBA or, if the GLBA is not applicable to a particular data provider, pursuant to the FTC's Safeguards Rule (§ 1033.311(d)(2)). The proposal further requires data providers to block a third party from accessing the interface "by using any credential that a consumer uses to access the consumer interface" (§ 1033.311(d)(1)). And, as a further step towards assuring security, the proposal permits data providers to provide authorized third parties with tokenized account numbers rather than actual numbers (§ 1033.211(c)). We support each of these provisions.

We also would support a further provision that permitted data providers to preclude a third party from accessing data with respect to covered consumer financial products or services outside of the developer interface by using a consumer's log-in credentials. Additionally, the Bureau could require third parties, as part of the authorization process, to commit not to attempt to access data regarding a covered product or service using a consumer's log-in credentials. The Bureau could potentially go even further and permit data providers to block the use of such credentials with respect to other consumer financial products and services if, in accordance with a qualified industry data standard, a data provider allowed tokenized access to data regarding such products or services either through screen scraping using the token or through a data interface made available at no cost and on a nondiscriminatory basis to third parties who obtain appropriate authorization from the consumer. If the Bureau were to proceed down this path, it should make clear that it would be problematic for financial institutions to block screen scraping using log-in credentials for data with respect to consumer financial products or services that fall within the ambit of § 1033 but are not covered by the current rule unless the financial institution made such data available on a tokenized basis.

Security of Third Party Data Systems:

The proposal requires a third party, as part of the authorization process, to commit to "apply to its systems for the collection, use and retention of covered data an information security provision that

[23] *CFSI's Consumer Data Sharing Principles, supra* n.1, at 1.

satisfies the applicable rules issued pursuant to [GLBA]," or, for entities not covered by GLBA, that satisfies the requirements of the FTC Safeguards Rule (§ 1033.421(e)). This parallels the obligation placed on data providers and we support this provision.

Additionally, under the proposal, data providers can "reasonably deny[] a consumer or third party access to an interface … based on risk management concerns" (§ 1033.321(a)). The proposal goes on to state two sub-rules that seem to point in opposite directions: first, "a denial is not unreasonable if it is necessary to comply with section 39 of the Federal Deposit Insurance Act or section 501 of [GLBA] (§ 1033.321(a)); and second, "To be reasonable.. a denial must, at a minimum, be directly related to a specific risk of which the data provider is aware, such as a failure of a third party to maintain adequate data security, and must be applied in a consistent and non-discriminatory manner" (§ 1033.321(b)).

Although we support the general principle of permitting data providers to deny access to third parties with respect to bona fide "risk management concerns," we are concerned about the absence of any definition of "risk management concerns" or "specific risk" in the proposed rule. This concern is heightened by the discussion of these provisions in the section-by-section analysis. Specifically, the NPRM, after noting the obligation of depository institutions to operate in a safe and sound manner, goes on to state that "The prudential regulators have issued guidance explaining that, to operate in a safe and sound manner, banking organizations must establish practices to manage the risks arising from third party relationships," including guidance as to the due diligence expected of depositories "before selecting and entering into third party relationships." The guidance articulates the rationale for that expectation as follows:

> Whether activities are performed internally or via a third party, banking organizations are required to operate in a safe and sound manner and in compliance with applicable laws and regulations. A banking organization's use of third parties does not diminish its responsibility to meet these requirements to the same extent as if the activities were performed by the banking organization in house.[24]

In certain circumstances, data aggregators are selected by a bank to act as a service providers to the bank. For example, many banks offer PFMS to their customers and contract with an aggregator to obtain data from other data providers about their customers' accounts with those other providers.

[24] 88 FR 37920, 37927 (June 9, 2023).

Banks also may use aggregators to assist in moving data between constituent parts of the bank. Similarly, many fintechs that, in some contexts, qualify as third parties under the rule also partner with banks to originate and service consumer financial products or services for the bank; for example, Upstart reports that it works with over 100 banks in originating consumer loans made in the name of those banks. In these instances, the prudential guidance regarding managing the risks arising from third party relationships would be directly applicable since the aggregators and fintechs are providing services to the banks.

But when a "third party"--be it a data aggregator or fintech engaging directly with a data provider – obtains data on behalf of a consumer with the consumer's consent, the third party is not providing services to or for the banking organization nor is the banking organization "selecting" the third party. Rather, in this context the third party is acting as the "agent" or "representative" of a consumer – indeed is deemed by the Dodd-Frank Act to be one and the same as the "consumer"[25]--in enabling the consumer to exercise their statutory rights under § 1033. And, as the NPRM repeatedly recognizes, the banking organization's interests may run directly contrary to the interests of the consumer (including the third party representative).

Thus, while a data provider unmistakably has an interest in assuring that data obtained through its developer interface is held in secure systems by third parties, we do not believe that data providers should be expected, e.g., to oversee the third parties' performance of the services it provides to consumers or third parties' compliance with applicable laws. Nor do we believe that a data provider should be permitted to deny access to data to a third party because, e.g., the data provider questions the third party's compliance with various consumer protection laws or because the third party has not committed to immunize the data provider in the event of a data breach. Thus, we urge the Bureau, in collaboration with the prudential regulators, to make clear the limits of data providers' legitimate risk management concerns with respect to the activities of third parties acting as representatives of consumers, and specifically to limit the focus to data security issues and not to broader and more open-ended "risk management" considerations.

In addition to the provision authorizing data providers to deny access to a third party based on risk management concerns, the NPRM also allows data providers to deny access if the "third party does not present evidence that its data security practices are adequate to safeguard the covered data" (§ 1033.321(d)). Here, too, we are concerned about the absence of any specification of the type of

[25] 15 U.S.C. § 1004(4) defines the term "consumer" to mean "an individual or an agent, trustee or representative acting on behalf of an individual."

"evidence" a data provider may require with respect to the adequacy of a third party's data systems. That concern is heightened by the NPRM's statement that even if a third party presents evidence that its data security practices "are adequate to safeguard the covered data," a data provider may "either grant access or perform additional due diligence on the third party as appropriate."

This statement is problematic in two respects. First, it could lead to long delays between the time a third party presents its evidence as to the adequacy of its security practices and the time the third party is permitted to access the data provider's developer interface. Such delays seem especially likely for smaller data providers who may not have the bandwidth to conduct due diligence on a large number of third parties simultaneously, but even large financial institutions may find it necessary (or in their interest) to extend the due diligence process and delay providing access to covered data. Second, allowing each data provider to conduct its own separate due diligence process could swamp third parties with a large volume of overlapping requests, each requiring slightly different information. Again, this risk looms especially large for smaller third parties.

To avoid these consequences, we urge the Bureau to specify the types of evidence that, if presented, would establish the adequacy of a third party's security system, and obligate the data provider to grant access without further due diligence. For example, in a related context the Bureau previously has indicated that it would rely on certification by an independent assessor that a security system complied with the Safeguards Rule if the certification met certain requirements, including an attestation that the assessment was conducted "by a qualified, objective, independent third-party individual or entity that uses procedures and standards generally accepted in the profession…"[26] The Bureau similarly could provide that data providers should treat such assessments as conclusive as to the adequacy of a third party's data security system. Alternatively, the Bureau could allow a standard setting body recognized by the CFPB as an issuer of qualified industry standards to establish a qualified industry standard for determining the type of data security certification that suffices to establish the adequacy of a third party's data security system.

In response to the Bureau's question, we do not believe the Bureau should require third parties to present a particular type of evidence such as an independent assessment; rather, as explained above, we believe the Bureau should require data providers to accept evidence of a defined quality if presented. The approach we recommend would create a strong incentive for third parties to

[26] *See* 2017 Payday Rule § 104.11(b)(6),(7), 82 FR 54472, 54883 (Nov. 17, 2017) (defining procedures and criteria for creating "registered information systems" to which covered lenders would be required to furnish data on covered loans and from whom lenders would be required to obtain a report before making covered loans).

obtain evidence in the form that would enable them to avoid further due diligence without imposing a legal straitjacket.

Finally, to the extent the final rule leaves data providers free to conduct due diligence either in general or absent the presentation of certain types of evidence from a third party, we urge the Bureau at a minimum to specify that data providers can conduct only reasonable due diligence, including a requirement that the data provider respond to a third party's request for access to a developer interface within a specified period of time after receiving information reasonably requested from the third party.

E. Minimization (§ 1033.421(a),(f),(h))

The final principle that FHN has espoused for a data sharing regime is that "Only the minimum amount of data required for application functionality are collected, and the data are stored for the minimum amount of time needed."[27] The proposal implements this principle by requiring a third party to agree to "limit its collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service" (§ 1033.421(a)). The proposal goes on to identify certain permitted (primary) uses including "servicing or processing the product or service the consumer requested" (§ 1033.421(c)(3)). And, subject to the general limitation stated in proposed § 1033.421(a), the proposal allows a third party to share data with other third parties who agree to abide by that limitation (§ 1033.421(f)). We are generally supportive of these provisions but suggest two clarifications and one important modification.

First, we do not think that the phrase "servicing or processing" adequately captures the ways in which third parties may need— and be expected by consumers--to use covered data in connection with the product or service the consumer has requested. For example, a consumer seeking credit from a third party may authorize the third party to access data to assess the consumer's ability to repay the contemplated loan and the third party may, in fact, deny a credit application if the data suggest that a particular consumer lacks the ability to repay a requested loan. Although such activity could be viewed as "servicing or processing the product or service the consumer requested," that is not a natural way to describe the underwriting process. We suggest revising proposed §

[27] *CFSI Consumer Data Sharing Principles, supra,* at 4.

1033.421(c)(3) to read "Assessing the consumer's eligibility for or delivering, servicing or processing the product or service the consumer requested."[28]

Second, the rule stated in § 1033.421(f) regarding sharing with third parties does not appear to leave room for use cases in which a consumer authorizes a third party to obtain the consumer's financial data for the very purpose of sharing that data with others. For example, Self Financial offers consumers the ability to build credit by enabling Self to access data from a consumer's transaction account, identify rent, cell phone, and utility payments, and report those payments to the national consumer reporting agencies. When Self reports those data to the NCRAs, the data gets incorporated into the consumer reports maintained by the NCRAs, and then can be further distributed to those with a permissible purpose under the FCRA to obtain a consumer report. Self is one of a number of companies offering similar services.[29] And Experian itself offers a similar product, Experian Boost, although the data that Experian accesses is incorporated only into Experian's consumer reports. It is difficult to see how products such as these could continue to function if, when a consumer permissions a third party like Self or Experian to obtain data, those data can be transmitted to downstream third parties only if such parties agree to limit their use of the data to "what is reasonably necessary to provide the consumer's requested product or service" (§ 1033.421(a)). To accommodate these use cases, a special rule is needed where the "consumer's requested product or service" constitutes reporting of data.

Third and finally, we recommend that the Bureau narrow the prohibition on data retention contained in § 1033.421(a) and reinforced in § 1033.421(h)(3) so that, if authorization for further collection is terminated or expires, the third party can retain a de-identified or pseudonymized version of covered data lawfully obtained prior to the point of termination/expiration and can use such data for permissible "supplemental primary uses" and permissible "public secondary uses" as previously defined, i.e., for analytics to improve the product or service for which the data was originally obtained or for bona fide research purposes. If each time an authorization terminates or lapses the third party loses the ability to learn from the experience in serving the consumers for whom data can no longer be obtained, cash flow underwriters and providers of personal financial management services would be severely handicapped in their ability to continuously refine their models or algorithms. Similarly, if the termination or expiration of authorization to collect data were

[28] As discussed in Part II, we also believe that using consumer-permissioned data to analyze or improve the product or service that the consumer requested constitutes a primary use, and thus we suggest that these terms be incorporated into §1033.421(c)(3).

[29] For a compendium of such companies *see* Kochran & Stegman, Utility, Telecommunications, and Rental Data in Underwriting Credit Reporting (2021).

to require historical data to be erased, the research community would be limited to studying the experiences of those who are continuing users of a given product or service. That would introduce a large selection bias into any research and make it all but impossible to research how consumers have been impacted by the various products or services they may have used.

As previously discussed, to the extent the Bureau is concerned about privacy risks that can arise from de-identified or pseudonymized data, there are steps the Bureau can take to mitigate those risks, but a blanket prohibition on retaining such data is, we submit, unnecessary and overbroad.

Conclusion

The Financial Health Network appreciates this opportunity to comment on the proposed rule. The promulgation of a final rule implementing § 1033 with respect to the covered products will represent a large and important step forward in providing consumers with access to data that can be used to help them more effectively manage their financial lives and improve their financial health. We look forward to working with the Bureau in any way that would be helpful in achieving this end.