COMMENT OF THE FINANCIAL HEALTH NETWORK
ON THE
OUTLINE OF PROPOSALS AND ALTERNATIVES UNDER CONSIDERATION
REQUIRED RULEMAKING ON PERSONAL FINANCIAL DATA RIGHTS
January 25, 2023

The Financial Health Network is pleased to have the opportunity to comment on the Outline of Proposals and Alternatives Under Consideration put forth by the CFPB as a preliminary step in what the Outline terms a "required rulemaking on personal financial data rights." We hope these comments will help the Bureau better define how data rights can be implemented to maximize the benefits to consumer financial health while minimizing the risks to consumers and the expense to data providers and third parties – a term the Outline seems to use to cover both aggregators and the ultimate authorized recipients/users of financial data.

The Financial Health Network's Interest in Financial Data Rights and Its Use of Consumer-Permissioned Financial Data

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. FHN has invested nearly two decades in developing tools to measure financial health and in uncovering what works to shape meaningful improvements in people's financial lives, particularly those that are most vulnerable.

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 for enabling research to better understand the state of financial health, FHN has been actively engaged on the issues raised by the Outline 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 which predated the Bureau's own principles, and have since published several widely-cited research reports on this topic[3].

---

[1] October 20, 2016: "Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration;" viewable at: https://finhealthnetwork.org/research/consumer-data-sharing-principles-a-framework-for-industry-wide-collaboration/

[2] September 2017, "Liability, Transparency, and Consumer Control in Data Sharing," at https://cfsi-innovation-files-2018.s3.amazonaws.com/wp-content/uploads/2017/09/27001532/2017_Liability-Transparency-Control-in-Data-Sharing_Full.pdf

[3] For Example: June 30, 2021: "Financial Data: The Consumer Perspective;" viewable at: https://finhealthnetwork.org/wp-content/uploads/2021/04/Consumer-Data-Rights-Report_FINAL.pdf ; October 2, 2020, "Consumer Financial Data: Legal and Regulatory Perspective," viewable at https://cfsi-

Beyond our role as a thought leader in this area, through its Financial Solutions Lab FHN has invested in and helped to nurture several innovative financial technology companies that rely on consumer-permissioned financial data to deliver services to consumers to help them advance their financial well-being. In addition, 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 response data 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 these comments.

Introduction

The prospect of a rule to implement consumer financial data access rights as envisioned in Section 1033 of the Consumer Financial Protection Act is a welcome one and one for which we have long advocated. In 2010, when § 1033 was enacted, the primary way in which consumer-permissioned data was being used was to power tools like mint.com that enabled consumers to link their transactional, savings, credit, and investment accounts in order to construct as complete a picture as possible of the household's financial position. But the impetus for § 1033, as we understand it, was the work of Professors Thaler and Sunstein, who recognized that as financial (and other) services have evolved, incumbent providers often know more about the usage patterns of their customers than the customers know about themselves. Thaler and Sunstein thus envisioned the possibility of consumer-permissioned transactional data being used to power apps that ingest such data, as well as more publicly-available information regarding the pricing of competitive products, in order to empower consumers to find a provider whose product and pricing best serves an individual consumer's needs.[5]

---

innovation-files-2018.s3.amazonaws.com/wp-content/uploads/2020/10/14142025/Financial-Data-White-Paper-_-1013_fin.pdf

[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 uses survey and transactional data in our research.

[5] In their book, *Nudge* (Yale University Press, 2008), Thaler and Sunstein advocate for modest governmental interventions in the form of RECAP (choice engines that Record, Evaluate, and Compare Alternative Prices). Such interventions (pp. 93-94) combine consumer-accessed usage data and mandated electronic pricing disclosures from product providers to enable consumers to better understand their current usage costs and their likely future costs of using alternative products. The authors provide examples of how RECAP would work for cellphones (93-94), prescription drug insurance (173-174), and credit cards (143-144), among other products. In *Nudge: The Final Edition* (2021), the authors rebrand RECAP as "smart disclosure" (142).

Although the Thaler-Sunstein vision has yet to be fully realized, in the fifteen years since *Nudge* was published consumer-permissioned data access has skyrocketed. That has, in turn, permitted third party service providers to introduce important new products that have, among other things, broadened access to affordable credit through cash flow underwriting; enabled consumers to move money cheaply and rapidly from person to person; and assisted consumers in managing their money and improving their day-to-day financial lives by, e.g., optimizing bill payments, automating savings, and avoiding costly overdrafts. At the same time, consumer-permissioned data has enabled researchers (including FHN itself) to use transactional data to build deeper insights into consumers' financial lives and the impact of various products on financial health.

To cement these gains, and remove the pain points that have emerged in the data sharing ecosystem, a § 1033 rulemaking is essential.[6] The Bureau's Outline is comprehensive and thoughtfully addresses the myriad of legal, economic, and technological issues implicated by the task of formalizing a regime of permissioned data access for consumers and the third party services on whom they rely. The transition from screen scraping to forms of access that do not require consumers to share their personal account access credentials is particularly complex, as it may involve substantial investments on the part of data providers and third party data recipients of all sizes, as well as data and technological standards that may be best left to Industry and other stakeholders to develop.

At the same time, we agree with Director Chopra as to the importance of avoiding "writing complicated rules to fit existing business models"[7] and instead "to provide[e] basic bright-line guidance and rules that can withstand evolution of the marketplace over time."[8] That seems to us especially important in this area given the speed of change in the types of products offered by financial institutions; the types of data they hold; the uses to which such data can be put to benefit consumers; and the technology through which such data can be accessed, analyzed, and utilized.

---

[6] For a brief summary of shortcomings in the current consumer financial data-sharing ecosystem, see our September 2022 paper, "Seven Pain-Points in the Consumer Financial Data Ecosystem: Priorities for the CFPB's Rulemaking Under § 1033 of the Dodd-Frank Act" downloadable at: https://finhealthnetwork.org/research/seven-pain-points-in-the-consumer-financial-data-ecosystem/

[7] See "Director Chopra's Prepared Remarks at Money 2020," October 25, 2022; viewable at: https://www.consumerfinance.gov/about-us/newsroom/director-chopra-prepared-remarks-at-money-20-20/

[8] See "Rethinking the Approach to Regulations," June 17, 2022; viewable at https://www.consumerfinance.gov/about-us/blog/rethinking-the-approach-to-regulations/

This comment letter addresses those aspects of the Outline—and choices the Bureau faces—that, in our view, have the greatest bearing on the future infrastructure's ability to support both data-based services that foster greater financial health, and continued innovation and development of such services. In Part I we address coverage questions including both the scope of covered data providers and of overed data. Part II addresses aspects of the Outline that would impose duties on data providers and correlative rights on consumers. We then discuss in Part III aspects of the Outline that would define the processes by which consumers can authorize (and deauthorize) third parties to access data on their behalf. Finally, Part IV focuses on aspects of the Outline that speak to the obligations of such authorized third parties.

We have not attempted in any of these sections to answer every question posed in the Outline, many of which require technical expertise and experience we cannot claim. Nor, in responding to proposals in the Outline or offering our own suggestions, have we attempted to carefully parse any limits that may exist on the Bureau's rulemaking authority to "administer and carry out the purposes and objectives" of § 1033 and other Federal consumer financial laws.[9] We believe, however, that it is possible to implement § 1033 in a way that delivers on its promise without pressing against the limits of the Bureau's authority and potentially leading to time-consuming litigation.

I. The Scope of the Rule

In this Part we discuss what data providers should be covered by the rule that the Bureau proposes following the SBREFA process and what types of data such data providers should be required to make available.

A. Covered Data Providers (Outline III-A)

On its face, § 1033 grants consumers the right to obtain data from any "covered person." The Outline, however, applies only to a subset of such persons. We agree that an initial § 1033 rule should not attempt to address the entire waterfront of covered persons, which implies that there will be subsequent implementing rules. Although such rules could, in theory, simply expand the scope of covered data providers without changing any of the substantive and procedural rules previously adopted, we assume that these subsequent rulemakings will also afford the Bureau the opportunity to build upon and refine the framework established in this initial rulemaking. That, in turn, means that the Bureau may face tradeoffs as it proceeds

[9] 12 U.S.C. § 5512(b)(1).

through this rulemaking between comprehensiveness and speed of execution and implementation.

We concur with the Outline's inclusion of Reg. E transaction accounts and Reg. Z credit card accounts as an important starting point for implementing § 1033. By and large, these are products used with greatest frequency and often present the greatest number of day-to-day decisions consumers must make. Further, they offer consumers and their service providers the richest vein of data on what income comes in and what expenditures go out. For better or worse, these products (in the form of funds availability policies, overdrafts, and revolving credit) represent how the vast majority of Americans who are subject to periodic liquidity challenges manage to cope with them. And these products involve complex pricing, with a combination of upfront fees and, for credit cards, interest rates, as well as back-end fees, such as overdraft, NSF, and late fees, all of which make it difficult for consumers to assess their current costs, or anticipate future costs of usage.[10] Not surprisingly, timely data on account flows, balances, and fees has for some time fed third party products that help consumers better manage cash flows and lower their costs of using these financial services and has enabled broadened access to credit, especially for those lacking or under-valued by standard credit scores.

Recognizing that there is more coverage yet to come through subsequent rulemakings, we nonetheless urge the Bureau to expand the proposed scope of coverage in its initial§ 1033 rulemaking in two respects in order to better advance financial health.

First, we believe that the rule that the Bureau proposes should cover providers of data with respect to certain other forms of consumer credit beyond credit card accounts.

For most consumers their largest obligations – and for many their largest monthly expenses – are their mortgages, auto loans and student loans. Mortgages and auto loans are often procured through third parties (i.e. mortgage brokers and auto dealers) whose interests are not necessarily aligned with their customers' interests and who may, as a result, sell high-cost

[10] For example, one former credit card executive recently commented: "[A]... typical credit card solicitation in the United States has more than 20 separate price points in it. So separate numbers that influence how much a person is going to pay in totality. So this is a pretty complicated product. And I think it's just impossible for anybody to juggle all those numbers. I don't care how smart you are, how good you are at math, like it just is very challenging." From "Holding Up a Mirror to the American Debt Machine with Elena Botella;" Episode #68 of the *How to Lend Money to Strangers* Podcast hosted by Bendan LeGrange. Transcript viewable at https://www.howtolendmoneytostrangers.show/episodes/episode-68

products. Similarly, while most student loans are obtained from the federal government, they are serviced by private servicers whose interests are rarely aligned with those of borrowers in obtaining the lowest-cost payment plans. Providing financial data rights with respect to these products thus can help stimulate competition and improve consumers' financial situations in ways similar to those that Thaler and Sunstein envisioned.

One of the companies in FHN's Financial Solutions Lab provides a clear case in point. Summer is a certified B corporation that partners with organizations to empower their populations to navigate and reduce student loan debt.[11] To do that, Summer needs accurate data about each borrower's current loan terms and payment plan. Unless the § 1033 rule covers providers of student loan data, the only way Summer could obtain the data it needs would be through screen scraping. And if student loan servicers are left outside the rule, they may feel empowered to do what they can to block such data access.[12]

More generally, access to data about these major financial obligations is critical for many personal financial management (PFM) apps. The goal of these apps is to help consumers manage their day-to-day finances effectively – to assure that they have sufficient money available to cover required payments and to optimize discretionary payments to reduce their debt burdens over time. Although transactional data from checking accounts can be used to identify and anticipate forthcoming bills, to best serve their customers PFM apps need to understand, for example, the size of outstanding balances and the interest rates consumers are paying on their various loans. That, in turn, requires access to data from the providers of these loans.

Importantly, student loans, mortgages and auto loans are each serviced by a highly concentrated group of large entities.[13] It would thus be relatively easy to include these

---

[11] https://www.meetsummer.org

[12] This risk is heightened by questions that apparently have been raised as to whether the Family Education Rights and Privacy Act, which in terms safeguards the privacy of "educational records" that are "maintained by an educational agency or institution,"20 U.S.C. § 1232(g), privileges student loan servicers to block consumer-permissioned access to student loan data.

[13] For example, in its Larger Participant Rule for nonbank Student Loan Servicers, the Bureau estimated that the top seven servicers covered by the rule were "responsible for between approximately 71 and 93 percent of activity in the nonbank student loan servicing market." (12 CFR Part 1090 [Docket No. CFPB-2013-0005]; RIN: 3170-AA35 at 47). Similarly, the Bureau's November, 2019 "Data Point: Servicer Size in the Mortgage Market" estimated that large servicers, those responsible for at least 30,000 loans each– were responsible for servicing 76 percent of all mortgages. And in its 2014 Larger Participant Rule for nonbank auto lenders, the Bureau estimated that the top 15 non-bank auto lenders accounted for "86

products in a rule while excluding or limiting the obligations of smaller entities and still enable a majority of consumers to permission access to these data.

Although we believe that eventually § 1033 coverage should be expanded to the full panoply of consumer credit products, given the myriad of other product types, the large number of providers, and some challenging boundary-line questions in defining what constitutes credit, we believe such expansion should be deferred to a later rulemaking. (Even if the proposed rule were limited to credit cards and Reg. E transaction accounts the Bureau may face some boundary questions regarding, e.g., buy now, pay later products which at least arguably meet the definition of a Reg. Z credit card notwithstanding the fact that these loans are repayable in four installments without a finance charge.)

Second, we believe that the rule the Bureau proposes should cover persons that issue access devices or provide electronic fund transfer services for certain accounts that are not covered by Reg. E.

The Outline appropriately proposes to cover institutions that directly or indirectly hold asset accounts covered by Reg. E and persons that issue an access device and provide EFT services with respect to such accounts. But because of holes in Reg. E, this excludes other types of transaction accounts as to which financial data rights can play an important role in improving consumers' financial lives.

Consider first accounts that fall outside of Reg. E because the accounts hold means-tested government benefits, the most important of which are accounts established to deliver Supplement Nutrition Assistance Program (SNAP) benefits. These benefits are accessed through what amounts to a closed-loop prepaid card system onto which money is loaded on a monthly basis. At the center of this system are a small number of private entities that issue access devices to these benefits and process payments from these accounts. The data they hold is critical to the lives of recipients since it shows, among other things, how much a consumer has spent at any moment in time and how much remains in the account.

Propel, another company in FHN's Financial Solutions Lab, has developed an app that helps users manage their SNAP benefits and save money.[14] It depends on access to data held by these SNAP payment processors. Unless the § 1033 rule covers them, Propel's ability to access

---

percent of market activity" of all nonbank auto lenders. (CFR Parts 1001 and 1090 [Docket No. 2014 - 0024] RIN: 3170-AA46 at 73). We believe bank and credit union auto lenders are somewhat less concentrated, but that the largest lenders still command significant market shares.

[14] https://www.joinpropel.com/

data via screen scraping may be blocked. Because these payment processors are indisputably "providing payments … processing products or services" to consumers, including "processing or storing financial … data for a[] payment instrument," they are thus covered persons within the meaning of the Dodd-Frank Act and can—and should -- be covered by the Bureau's rules.[15]

The same is true for those responsible for administering flexible spending accounts and health savings accounts. Consumers who sign up for such accounts agree to have money deducted from their paycheck and set aside to cover eligible health or other qualified expenses. We are uncertain as to who is the custodian of those funds (and thus a covered person by virtue of providing such custodial services). But in all events it is clear that the companies engaged to administer these programs, who generally arrange for consumers to obtain a debit card that can be used to make qualified expenditures and who process reimbursements are, like the SNAP administrators, engaged in providing processing products or services to a consumer and in storing financial data for a payment instrument. And, the data that these processors hold can be valuable to consumers in managing their financial lives. These processors, then, are covered persons who can, and should, be covered by the Rule.

B. Covered Data [Section III-C of the Outline]

We address here the types of information listed in the Outline as potential categories that the rule the Bureau proposes would require covered data providers to make available to consumers and authorized third parties.

Periodic Statement Information and Information Regarding Transactions Not Yet Settled (Outline Section III(C)(1)(i),(ii)) Generally, a great deal of innovation has come from information that the consumer is already able to obtain directly through providers' web-portals and through electronic statements. Thus, we agree with the Outline that the proposed rule should require access to data that generally appears on periodic statements along with data regarding initiated but not settled transactions (both debits and deposits) – data that already is available through many banks' web portals. They represent the consumers' cash flows and net borrowings. These, also, based on other regulations already in place, include fees (such as late fees on credit

[15] 12 U.S.C. 1002(6), 15(A)(vii)

cards and fees on overdrafts both of which must be disclosed in the month or period assessed and cumulatively[16]), finance charges (again as assessed and cumulatively), APRs and APYs.[17]

Online Banking Transactions That Have Not Yet Occurred: We also agree with the Outline that the proposed rule should cover online banking transactions that have not yet occurred. **(**Section III-C-1-iv in the outline.)

Most institutions' online banking services permit a consumer to initiate payments to merchants via ACH on a "push" basis. Consumers who use such "push" bill payment services provide the relevant information to their bank about their accounts with all the merchants to whom they initiate such payments when they use the service. When such a consumer wants to switch their checking account to another bank, they must generally recreate this information at their new bank, entering the merchant account information one-by-one. This presents a barrier to account switching. Thus we believe it would foster competition if financial institutions hosting checking accounts were required to provide such information in machine readable form to third parties, including potential competitors. With their new bank supplied with the merchant's information in electronic form, the consumer could begin initiating at their new bank the same bill payments they had habitually initiated at their old bank without having to set up each merchant manually. (Of course, this would not reduce the friction involved in redirecting pull payments or direct deposits and thus enable true account portability, but doing so seems beyond the scope of § 1033 and certainly beyond the scope of an initial § 1033 rulemaking.)

It is our understanding that most banks rely on one of a small handful of vendors who provide such "consolidated bill payment services" (as opposed to "biller direct" bill payments, i.e., pulls, that consumers initiate or pre-authorize at billers' web sites). These vendors maintain for each consumer a "biller list" consisting of the consumer's account number with each merchant to which the consumer makes payments. We believe such information is, at a minimum, "in the control" of the data provider within the meaning of § 1033 and that banks should therefore be required to share such information in machine readable form; this would only require that

---

[16] The Outline specifically calls out disclosure of overdraft and NSF fees on a calendar year-to-date basis but is silent about credit card late fees even though they also must be disclosed cumulatively. *See* 12 C.F.R. 1026.7(b)(6)(iii)

[17] We are sensitive to the concerns that some have expressed about the security risks inherent in requiring electronic, machine-readable access to transaction account numbers. On the other hand, some PFM apps – for example, those that allow for automated savings or money transfers – need the ability to withdraw or deposit funds to deliver the product or service the consumer has signed up to receive. We lack the expertise to assess whether this can be done efficiently through tokens rather than the exchange of account numbers.

banks direct the relevant vendors to establish file exchange protocols among themselves for transferring this limited information.

We further believe there would be minimal security risk to consumers, data holders, or billers in sharing consumers' biller account numbers across institutions, as such information cannot be used to access the consumer's assets or to obtain assets of the biller (e.g. prior payments received by the biller).

Other Data Categories: We have some misgivings about several of the other categories of data covered in the Outline. Although we admittedly are not expert in these areas, we fear that they would bring the Bureau into more unchartered water – both legally and technologically – and create more cost and implementation delay than may be warranted, especially for an initial § 1033 rule. We briefly address each of these categories:

- **"Other information about prior transactions not typically shown"** (Section III-C-1-iii in the outline). For the vast majority of transactions, we do not see substantial benefit in requiring access to information about the interbank routing of transactions such as the account number and routing number of the payee on a bank or credit card transaction. Only for those transactions that are fraudulent or disputed do we see potential value in such routing information as, in those cases, the data could have value to the consumer in pursuing a dispute and, potentially, to third parties in preventing future transactions, However, we are concerned that those data may not always reside in the same systems of record that are used to compile periodic statements or feed consumer-facing web portals; to the extent that is true, it may be difficult for the FI to recover the information (certainly in any automated or instantaneous fashion) without significant infrastructure development cost. Moreover, we see potential security risks in requiring access to certain data fields such as the bank account numbers of each and every payee. These costs and risks may outweigh the benefit of requiring access to payee information, especially since we believe that most financial institutions would provide this information to a customer voluntarily on request where the customer was seeking to recover a payment that was misdirected or trying to track down a payee that defrauded the consumer. To the extent the Bureau is concerned that in such cases data may not be forthcoming, we believe the better solution would be to amend Regulation E to require that the institution provide such information upon a consumer's request in support of the consumer's own recovery efforts.[18]

[18] If obtaining payee information with respect to recurring pull debit payments were useful in facilitating account switching, the case for requiring access to such information at least for this class of transactions would be

- **Account identity information. (**Section III-C-1-v in the outline.) Consumers provide financial institutions with a variety of personally identifying information when they are establishing accounts with the institutions. Some of this information is required or secured to satisfy "know your customer" requirements enumerated in the Bank Secrecy Act and other anti-money-laundering and anti-terrorism regulations—and institutions must verify it before establishing an account. Other demographic information can help the institution better understand a new customer's potential needs, although we note that Reg. B substantially limits the information that creditors – including credit card issuers and providers of overdraft services -- can collect from applicants regarding their race, ethnicity, national origin, religion, or sex.[19]

  As the Outline points out, what characterizes virtually all of this information is that, unlike information about their account history (such as transactions, balances, fees, and interest paid, etc.), account identity information, by definition, was supplied to the data provider by the consumer and thus is information that the consumer can supply to another financial institution at any time—and (with the likely exception of driver's license numbers which are not routinely captured by many financial institutions) most of it from memory. Thus, the potential benefits of an institution sharing account identity information with a permissioned third party are limited. Indeed, simply transferring information in company A's profile of a consumer to company B would bypass a potentially useful moment of friction (some would call it discretion) in which the consumer could be selective about what they divulge to a third party or have an opportunity to update information (like phone numbers, addresses, or marital status) that may have changed.

  There is, however, some potential value, as the Outline also points out, in enabling a third party that has been authorized to obtain access to data on behalf of a consumer from a particular account to match information supplied to the third party by the consumer with account identify information regarding the account to be accessed in order to verify that the individual claiming the right to access information with respect to that account is,

---

compelling. But it is unlikely that knowing the merchant's bank, account number and account name would be sufficient to avoid the burden of switching pre-authorized debits since the consumer (or the consumer's new bank) still would need to communicate to the merchants doing the pulling that the consumer wishes to cancel the prior standing debit authorization or initiate a new one from another account. Thus, we do not believe that requiring access to payee information even with respect to recurring pull debits will materially facilitate account switching.

[19] 12 C.F.R. 1002.5(b). FHN has previously urged the Bureau to reconsider these limitations and continues to believe such reconsideration is warranted. *See* "Financial Health Network Comment in Response to the Request for Information on the Equal Credit Opportunity Act and Reg. B," Dec. 1, 2020, https://www.regulations.gov/comment/CFPB-2020-0026-0124

indeed, an owner of the account. In principle it seems to us that this could be accomplished by requiring data providers either to provide access to account identity information or to confirm or deny key account identifier information such as address, date of birth, and social security number. We acknowledge, however, that we lack knowledge as to how such confirm/deny procedures work or can work in practice.

- **Other information.** The Outline (III-c-1-vi) asks about the benefits and risks associated with requiring a variety of other sorts of information to be provided with consumer permission to third parties under the rule the Bureau proposes. We have assessed these benefits and risks through the lens of improving consumer decision-making and financial health and share our thoughts below.

    - **Consumer reports obtained by the covered data provider.** We view such data as having limited incremental value while also potentially adding significant costs to covered financial institutions and raising prickly questions involving ownership rights. Consumers have the right to obtain free and current credit reports on their own through AnnualCreditReport.com or, in the case of an adverse action notice or accuracy dispute, directly from the credit bureau that supplied the information leading to the adverse action or involved in the dispute. Moreover, the "file disclosures" that consumers generally receive directly from CRAs contain information about the identity of furnishers (which enables a consumer to initiate a dispute with the furnisher) while the reports received by users do not. Thus we see limited, if any, incremental value in requiring that consumer report information obtained by a data provider – which may be quite stale by the time the consumer requests it -- should fall under the proposed § 1033 rule. Further, it is unclear to us whether these data reside in the same system of record that holds the transactional and other data from which periodic statements and online banking portal displays are generated, and thus including consumer report data within the rule may add cost and implementation delay. (In a subsequent rulemaking the Bureau may want to expand § 1033 coverage to include consumer reporting agencies so as to require them to provide the reports to which consumers are already entitled under the FCRA in a machine-readable format that consumers' can share with their third party agents.)

    - **Fees that a covered data provider can assess.** In describing the data elements included in the periodic statement category the Outline lists "the terms and conditions of the accounts, including a schedule of fees that may be charged." In the "other information" category the Outline also lists "fees that the covered data

provider assesses in connection with its covered accounts." It is not clear to us how the latter differs from the former.

We agree that fees that the covered data provider assesses an individual consumer in connection with the consumer's covered account should be included in the rule. But those fees –like finance charges -- should be reflected on monthly statements, either in sequence or in separate areas of the statement (such as reg DD's requirement to summarize year-to-date overdraft and NSF fees on a consumer's monthly checking account statement and Reg. Z's similar requirement with respect to certain credit card fees). Given that, and given that the full schedule of fees – which often includes dozens of fees that could be charged for services consumers may, but rarely do, request – are typically available on data providers' websites (and without requiring consumer-permissioned access), it is unclear whether the benefits of importing these fee schedules into data portals accessed on an account by account basis would be worth the cost.

- **Bonuses and rewards.** Bonuses, rewards, and other incentives -- such as cash back, frequent flier miles, other sorts of loyalty points, or discounts probably play an outsized role in consumers' selection and use of certain financial services, particularly among credit card transactors, and promotional rates on purchases and balance transfers may do the same for revolvers.[20] In our experience, where the card issuer itself manages the rewards program – as is true of cash back products and those offering issuer-created currency -- such rewards generally appear on periodic statements and thus could be enumerated as another sub-category of data covered by the requirement that the data provider make available data that generally appears in periodic statements.[21] Similarly, promotional interest rates likewise will appear on periodic statements. But there are a myriad of discounts that a credit card issuer may offer from time to time through online marketplaces or one-off arrangements with merchants and we question both the value and feasibility of requiring electronic, machine-readable access to all such discounts and incentives.

[20] A former credit card executive writes: "...rewards are only particularly valuable to consumers who pay their credit card bills in full every month–if a consumer isn't paying off their balance monthly, it is hard for them to have enough available credit to make most of their daily purchases on the card, and few rewards will ever accrue while interest piles up." In Elena Botella: *Delinquent: Inside America's Debt Machine;* University of California Press, 2022 at 149.

[21] We do not believe that card issuers generally have information on rewards earned in the currency of a co-branded partner such as airline frequent flier miles.

- **Security breach information.** We do not believe that information about breaches of the consumer's information at the data provider warrants inclusion under the rule. Obligations to disclose this information to consumers are already mandated in other regulations[22] . Such information is unlikely to be housed in the system of record from which periodic statement and online banking account data will be provided and thus requiring its disclosure may add cost and delay. Given that, and given that these data fall well outside what we see as the core purposes of § 1033, we do not recommend their inclusion.

Current and Historical Information: (Section III-C-3 in the Outline) To most effectively help consumers make choices about product selection and usage, and to help them manage their finances more generally, third party providers generally rely on multiple quarters of historical transaction detail from transaction, savings, and credit card accounts. Earnings and spending both fluctuate seasonally, and a consumer's earnings and costs of living--and their susceptibility to spikes and dips in either—are most discernible over a full year. Tax preparation and planning generally requires the last full year's worth of expense detail. So does planning—in the form of short-term savings—for lumpy but recurring expenditures (such as winter heating bills or back-to-school expenses in the fall).

We concur with the proposals that the Bureau is considering regarding historical information, namely to require a covered data provider to "make available information going as far back as far back in time as that covered data provider makes transaction history available directly to consumers." We believe that at least the large checking account providers make data available for the most recent 24 months of transactions. Likewise, we believe most credit card providers make details of prior transactions available to card providers on a similar basis.

That said, some institutions may make such transactional data available today for more limited periods of time or only in the form of .pdf files containing images of monthly statements. We do not consider such formats to be machine-readable in ways that would enable a third party to automatically discern or analyze transaction details such as date, dollar amount, merchant name and address, or merchant category. Thus we would urge the Bureau to explicitly require

[22] The Federal Banking Regulators (OCC, FDIC, Federal Reserve, and NCUA) have issued joint Interagency Guidelines Establishing Information Security Standards that interpret Section 501(b) of Gramm-Leach-Bliley Act. The Guidelines include provisions for customer notification in the event of "a security incident involving the unauthorized access or use of the customer's information" and spell out the content of the required notices. The institution may limit its provision of the notice "to those customers with regard to whom the institution determines that misuse of their information has occurred or is reasonably possible." See, for example: https://www.fdic.gov/regulations/laws/rules/7500-4750.html.

such historical data to be made available in the same electronic format as current data at least so long as the data provider has such data in a digitized format. We also urge the Bureau to establish a minimum standard for access to historical information so that consumers have a right to obtain at least 12 to 24 months of historical data even if a particular financial institution elects to provide less through its online portal.

II. Duties of Covered Data Providers

Under § 1033 covered data providers must make covered data "available to a consumer" – a term which, under the Dodd-Frank Act, is defined to include the consumer's "agent…or representative"[23] —"upon request" and in "an electronic form usable by consumers." The Bureau is directed to "prescribe standards … to promote the development and use of standardized formats for information, including through the use of machine readable files, to be made available to consumers under this section."

We agree with the Outline (III-D-2-i) that the duty to make data available is not discharged merely by enabling consumers to open a PDF or to download data into a spreadsheet. We also agree with the concerns expressed in the Outline about the risks inherent in screen scraping and thus support a rule that requires covered data providers – or, at a minimum, larger providers – to establish data portals from which covered data can be accessed without the use of log-in credentials. We likewise agree that the proposed rule should disallow, or at a minimum permit data providers to block, screen scraping from data holders who have established a portal is operational and properly functioning.

As the Outline suggests, we believe the proposed rule should be crafted to accommodate the interests of small entities who are covered data providers (and who would be dependent on their core processors to meet any data portal requirements). In our view, a phased implementation of the final rule holds promise as a means of reaching such an accommodation. Indeed, if the Bureau were to elect to expand the categories of covered data beyond those generally available through online bank portals and periodic statements, the Bureau may also wish to establish phased implementation dates for such additional data categories while allowing other elements of the rule to take effect.

Today, to the extent data sharing occurs without screen scraping, it is pursuant to bilateral agreements between individual data providers and data aggregators. That means that such data sharing exists as a matter of grace and is subject to the puts and takes of contract negotiation in

[23] 12 U.S.C. 5481(4).

terms of what data is shared, with what frequency, through what processes. A system dependent upon bilateral agreements also may make it more difficult for competitors to emerge in the market for data aggregation.

One of the important contributions that a § 1033 rulemaking will make, therefore, is, by its very nature, to substitute a system of *data rights* secured by federal law and not dependent upon private negotiations. In this regard, we do not believe the Bureau should permit data providers to both block screen scraping and also charge consumers directly or indirectly (through charges on aggregators or third parties) for accessing a data portal; permitting such fees would seem inconsistent with the statute's objective of enabling the free flow of consumer-permissioned data. Indeed, the idea of permitting such fees seems inconsistent with the very concept of data ownership and data rights embedded in § 1033.

As a corollary to the principle of a rights-based regime, we urge the Bureau to make clear in the rule it proposes that while data providers can provide data only to authorized representatives of the consumer (and thus must be provided with appropriate proof of the authorization before sharing data), data providers are not otherwise responsible for -- or empowered to -- police the authorized third parties' compliance with whatever duties the Bureau proposes to impose on third parties, including, for example, restrictions on data use, retention, security or accuracy. Data providers have their own self-interests that do not necessarily align with the purposes of § 1033 or the interests of consumers, and thus data providers should not be viewed as third-party beneficiaries of, or as policemen for, rules designed to protect consumers vis-a-vis their authorized third party representatives.

Of course, a rule that defines covered data as broadly as we have suggested and that requires that data be made available through data portals will require some rules of the road to determine what categories of covered data are made available to consumers' authorized representatives based upon the scope of the authorization or the purpose for which the authorization was granted (e.g. the nature of the product or service or the scope of a research project for which the consumer has enrolled). We discuss this further in Part IV below where we discuss limitations on third parties.

Additionally, we agree with the Outline (III-D-2-a) that the proposed rule should address data portal technical performance requirements, although here too we think that, at least for the initial § 1033 rule, a principles-based, policies-and-procedures approach, is preferable to an attempt to promulgate detailed, prescriptive standards. At a minimum, any data portal should be expected to achieve the same level of performance as the data holder's own mobile and online service portal offers its customers. We also agree with the Outline (III-D-2-b) that data providers should be free to exclude from a data portal any information they know to be false (although the risk of that occurring even in the absence of a rule seems quite low). And we

likewise believe that, if there is a risk of data being corrupted as it moves from a data holder's system of record to a data portal accessible to authorized third parties, data providers should have a duty to adopt reasonable policies and procedures to prevent such corruption from occurring (although again the risks seems quite low).

III. Obtaining and Retaining Consumer Authorization (Outline III-B-2, III-D-2-iii)

For a consumer to exercise their right to share their financial data with a third party acting on their behalf as envisioned under § 1033, the consumer must first grant permission to the third party to serve as the consumer's representative in obtaining the data. To be meaningful, such consent must be informed and must be easily revocable by the consumer. We thus generally support the Outline's attempt to establish authorization procedures that will facilitate informed consent and that will make revocation rights salient to consumers and easily exercisable.

At the same time, we urge the Bureau, in crafting the consent and revocation procedures of the rule it proposes to be sensitive to the self-interest of the various parties to the data ecosystem, including both data providers and aggregators; to the risk of information overload frustrating the goal of achieving informed consent; and to the risk of creating what Sunstein and Thaler colorfully term "sludge" – that is "friction that makes it harder for people to obtain an outcome that will make them better off (by their own lights)."[24]

Against this background we offer a few observations and recommendations.

- **Disclosure Content.** There is abundant evidence that in many contexts consumers today scroll through disclosures without reading them and simply click on the "I agree" button.[25] The risk of that happening likely increases with the length of the disclosures. Yet to the extent that the scope of the data that a third party can obtain and the future uses that third party can make of the data are controlled by the scope of the initial disclosures, third parties will be tempted to write prolix disclosures to cover the waterfront of potential useful categories of data or use cases, Thus, the Bureau will need to balance the interest in assuring that consumers understand how their data will be used against the interest in discouraging disclosures that obscure more than they inform. In this regard we note that electronic disclosures can include hyperlinks that enable those consumers who want to read more to do so while streamlining the information to which every consumer is exposed.

---

[24] *Nudge: The Final Edition* at 153.

[25] You're not alone, no one reads terms of service agreements

- **Authorization and Authentication Processes.** Ordinarily, in order to authorize a particular third party data user to obtain a consumer's data, the consumer first agrees to the third party's terms and conditions with respect to the product or service to be provided to the consumer. The third party will then redirect the consumer from its website to the website of an aggregator that will actually procure the data. The aggregator will secure the consumer's authorization to pull data from particular data providers. If the data providers in question provide data through a data portal – as will become the norm under the Outline's approach – once the consumer provides the aggregator with authorization, the aggregator will redirect the consumer to the website of the data provider where the consumer will log in with their credentials to authenticate the consumer's identity and ownership of the account(s) of that data provider from which data will be pulled. In today's world, in the absence of a rule designed to facilitate data access, the data provider may also require the consumer on its website to authorize sharing of particular categories of information. When that step is complete the consumer will be returned to the aggregator's site to confirm that the account linkage has been made and then to the data recipient's site to complete the enrollment/application. Each of these steps may require two-factor authentication. And if the consumer is permissioning access to multiple accounts held by different data providers the authentication (including the back-and-forth between aggregator and data provider) will have to be repeated multiple times before the consumer is returned to the data recipient's website.

  Needless to say, the potential for breakage in this process is inherently high. We urge the Bureau not to increase that risk by requiring or even permitting duplicative steps – for example, by requiring or allowing data providers to seek what would amount to a second authorization. As Thaler and Sunstein argue, ""the most basic principle of good choice architecture is our mantra: Make It Easy."[26]

- **Revocation of Access:** A system that makes consumers' right to revoke access salient and easy to exercise can relieve some of the pressure on dotting every "I" and crossing every "T" at the front end of the authorization process. We recommend that whenever a consumer uses a third party's product or service e.g. by logging into the third party's website, the third party be required prominently to remind the consumer of their ability to terminate their enrollment or "unsubscribe" and thereby terminate the consent to data access. We also believe that data providers should be free to remind

[26] *Nudge: The Final Edition* at 151.

consumers of the third parties that are accessing the consumer's data and provide a means by which the consumer can revoke access on the data holder's website with respect to any such third party provided that the data provider is required to promptly notify the third party of the revocation. And we also recommend that the Bureau consider establishing a finite period of dormancy (i.e., a period of a certain length of time during which a consumer enrolled in a service did not use the service—e.g. a year), after which the authorization would lapse and the third party service provider would be required to obtain the consumer's active re-authorization before continuing to access the consumer's data.[27]

However, we do not believe that a consumer who regularly or intermittently uses a third party service should be required to re-authorize the third party's access to their data at fixed intervals. Nor do we believe that consumers should be required to periodically reauthenticate themselves to the data holder. Such a reauthorization or reauthentication requirement – whether imposed by rule or by the actions of data providers -- would create the kind of sludge about which Sunstein and Thaler warn. Rather we urge the Bureau to propose a rule that specifies that a consumer's continued use of a service for which they have authorized access to their data serves as a *de facto* confirmation of their authorization and that, absent a change in account identity information, the consumer's initial authentication should continue.

- **E-Signatures:** Whatever disclosures and consents the Bureau elects to require before a would-be data user and its aggregator are authorized to obtain a consumer's data, it is essential that the processes for providing such disclosure and obtaining the requisite consent do not themselves serve as a barrier to data access or a means of entrenching incumbency. In this regard special consideration needs to be given to the E-Sign Act. Under that Act -- which was enacted in 2000 towards the dawn of the smartphone era and before the first tabloid was released -- before a required disclosure can be given electronically, the would-be recipient of the disclosure must first be provided with a notice of, among other things, (i) the "hardware and software requirements for access to and retention of" the electronic disclosure to be provided; (ii) the right to have the disclosure in paper form; and (iii) the consumer's right to withdraw consent to receiving future disclosures electronically and the procedures for doing so. The consumer must

[27] It seems comparatively less important to us to include information about revocation at the point of initial authorization. That is unlikely to be relevant to consumers at that moment in time nor likely to be remembered should the consumer decide they wish to revoke authorization. Mandating the inclusion of such information in the initial disclosure would seem to us to lean in the direction of information overload.

then consent to receiving the disclosure electronically and that consent must be given in a manner that "reasonably demonstrates that the consumer can access information in the electronic format that will be used to provide the required disclosure." Only after such notification has been given and consent received can the consumer be given a required disclosure, such as disclosures about the data that will be accessed and how it will be used.[28]

We are concerned that layering these requirements on top of a process that, as described above, is likely to involve multiple stages as the consumer moves (or is moved) from the site of the third party data recipient to an aggregator to a data provider and then back will create considerable friction that will disserve the goals of §1033. Fortunately, in enacting the E-Sign Act Congress expressly authorized agencies to exempt specific types of required notices from the consent requirements if the agency finds that "such exemption is necessary to eliminate a substantial burden on electronic commerce and will not increase the material risk of harm to consumers."[29] We believe that such an exemption is warranted in cases where a consumer proactively engages electronically with a would-be data recipient (whether by entering a URL address into a browser or clicking on a link) and where the consumer provides an email address signifying the consumer's ability to obtain information online.

Custody of authorizations and the role of data aggregators. Data aggregators currently play an essential role in the provision of consumer disclosures and the collection of consumer authorizations as well as in accessing the consumer's data. We expect that to continue under the regime contemplated by the Outline. Indeed we doubt that many of the entities that actually use consumer-permissioned data would be equipped to provide the disclosures required or to secure consumers' authorizations and to create linkages with data providers to authenticate the consumer and obtain a token with which data could be accessed. In any event, it would be inefficient to require each would-be data recipient independently to create such processes or to require data providers to engage separately with each third party data recipient. Accordingly, we recommend that aggregators be permitted to perform these functions on behalf of third party data recipients. However, we have some concern that the role these aggregator-intermediaries play might accord them unintended and unwarranted market power in the data-sharing ecosystem by imposing undue costs of switching aggregators on the

[28] 15 U.S.C. §7001(c)

[29] *Id.* § 7004(d)

part of the data recipient third parties. We therefore urge the Bureau to consider provisions in the rule it proposes that would mitigate that risk.

Specifically, we believe that the proposed rule should provide that an aggregator (who generally contracts with and is paid by the data recipient)[30] and who may transport, clean, and organize data on behalf of the recipient, should be viewed as a sub-agent of the consumer who is bound by the terms of the relationship between the consumer and the data recipient but not a party to it. In order to enable a competitive market for data aggregation services, we urge the Bureau to explore and implement ways to assure that a data recipient desiring to switch aggregators would be able to instruct its incumbent aggregator to transfer log-in credentials or tokens it received (from the consumer or the data provider associated with the consumer's account, respectively) to a competing aggregator so long as the affected consumers are given advance notification of the change in aggregators and afforded the opportunity to revoke their authorization prior to the transfer.

Such "permission portability" would enable a data recipient to switch data aggregators without requiring its customers to reauthorize access (through the new aggregator) to data about their accounts. In the absence of permission portability, such forced reauthorizations would be so costly to data recipients in terms of lost enrollments that data recipients would be effectively locked into their aggregator relationships.

IV. Third Party Obligations (Outline III-E-1)

Given the centrality of consumer consent to a data rights regime as discussed above, it necessarily follows that the data that a third party obtains and the uses to which those data are put must be constrained by the authorization provided by the consumer. Indeed, FHN has long advocated for the principle of "data minimization" as a limitation on the data that is obtained and retained. But in turning that principle into a concrete regulatory framework there are implications and potential unintended consequences that we urge the Bureau to carefully consider.

[30] Our Financial Solutions Lab's experience advising and supporting financial-health-oriented start-ups seeking to serve low and moderate income consumers has given us insight into the economics facing users of aggregator-sourced data. Where services rely on recurring access to transactional data, for example, aggregator subscription fees–typically structured on a monthly subscription basis per-customer-account-accessed-per month–constitute a major source of expense and one that is paid regardless of that customer's activity level or the amount of data accessed.

A. Limits on Collection (Outline III-E-1-ii)

We are in general agreement with the principle stated in the Outline (p. 41) that authorized third parties collection of consumer information should be limited "to what is reasonably necessary to provide the product or service the consumer has requested." We note only that not all authorizations will be for the purpose of obtaining a product or service and that therefore the rule the Bureau proposes should accommodate cases in which authorization is provided to, e.g., a researcher or government agencies to support research or market monitoring.

In the interests of "data minimization," various organizations such as the Financial Data Exchange (FDX) have attempted to define a set of use cases and the types of data required for each use case. We do not believe, however, that the Bureau should attempt by rule to codify use cases and the categories of data needed to satisfy each use case, if only because of the speed with which the market and product requirements change. Rather, we recommend that the Bureau's proposed rule adopt the general principle stated above with, perhaps, some illustrations of the principle (e.g. distinguishing a use case that needs to verify only a consumer's current available balance from one that depends upon receiving transactional data on a historical and/or recurring basis). The Bureau may wish at some point to provide a measure of deference, such as a presumption of compliance or potentially even a safe harbor, to industry standards defining use cases and the associated categories of data reasonably necessary for each use case. But, if so, the Bureau should first ensure that such standards do not unnecessarily restrict the flow of data or data-derived innovations. Thus, it should assure that such use-case standards are developed with meaningful input from consumers and their advocates and from third party data users–and that there are standard governance processes in place that allow for amending or re-defining use-cases as product needs evolve.

We likewise are in general agreement with – and support the adoption of – the Outline's further principle that would permit authorized third parties to access data only as "often as would be reasonably necessary to provide the product or service the consumer has requested" (although we again add the caveat that not all data authorizations are for the purpose of obtaining a product or service). But we feel the need to get granular about what a "reasonable frequency" might mean, particularly in the case of services designed to meet the needs of the most vulnerable—and often most liquidity-constrained—consumers.

Consider the most vulnerable consumers whose checking balances hover near zero. Research indicates[31] – and the experience of some of FHN's members confirms – that such consumers are the heaviest users of mobile banking services, checking their balances multiple times throughout the day. It is easy to imagine that such consumers are checking to see whether they have available funds to make a purchase—and how large a purchase they can make without overdrafting. In many cases they are checking to see whether a pending deposit has cleared, making new funds available for paying a bill or transferring money to a family member.

Third party services designed to help such consumers manage their daily cash flows and liquidity necessarily rely on similarly frequent data access. By regularly checking an account and either alerting the consumer to a change or automatically injecting funds in the account to provide short term liquidity (as in the case of a number of personal finance management apps that provide direct-to-consumer advances), these third party service providers free the consumer from having to check balances or transfer funds manually and they help the consumer avoid late fees and overdraft fees. The volume of data such services require from any query (e.g. the current account balance and any pending transactions) is low. The services' consumer value can be high. And their cost savings to the bank may be substantial to the extent they reduce the frequency with which their customers use other and potentially higher-cost channels for monitoring their accounts.

Thus, if the Bureau were to elect to do more than state a general principle regarding access frequency – either by providing illustrations of reasonable frequency or by imposing a numerical cap on the frequency with which data can be accessed – we would urge the Bureau to set such a cap at a high number, perhaps as high as 5 times per day or even once per hour, at least for the most demanding cash-flow management services provided by third party recipients of consumer data.

We are mindful that requiring data providers to maintain a data portal from which data can be called at such frequent intervals is not without costs. On the other hand, permitting such calls by third-party PFM services would likely reduce the frequency with which consumers would feel the need to log into their online banking portal to check the status of their account. Moreover, the costs of supporting data access must be placed in context, both relative to how consumers use online services, and the more costly telephone, ATM, and in-branch interactions

---

[31] *E.g.*, Curinos, "Competition Drives Overdraft Disruption" at 32-33 (2021), available at https://curinos.com/our-insights/competition-drives-overdraft-disruption/#:~:text=This%20research%20both%20confirms%20and,in%20overdraft%20policies%20and%20programs.

they replace. In all events, we believe these costs are justified by the benefits to consumers seeking help in managing their day-to-day finances.

B. Limits on Data Retention (Outline III-E-1-iv)

The Outline proposes to require third parties to delete consumer information "that is no longer reasonably necessary to provide the consumer's requested product or service or upon the consumer's revocation of the third party's authorization. This principle seems to us more problematic than the principles discussed above regarding data collection

To begin with, in some use cases it will be far from obvious when data is "no longer reasonably necessary" to provide a particular product or service. For example, a provider may deliver a product or service using an algorithm that uses up to x months of transactional history. Over time, however, the provider may discover that it can enhance its service by increasing the amount of historical data that it uses. More generally, as underwriting and predictions increasingly rely on artificial intelligence and machine learning, data retention can lead to advances that enable providers to better serve consumers. And, since there is no comparable deletion requirement with respect to data acquired through other channels or with respect to the very same data in the hands of the data holder, a deletion requirement would put data acquired pursuant to § 1033 in a disfavored position.

Beyond all this, long after a consumer's relationship with a provider ends, disputes can arise as to whether the provider met its obligations to the consumer. If a rule were to require that the data relevant to answering that question had to be deleted, such disputes would turn into he-said, she-said conflicts. Indeed, the CFPB's own ability to direct redress to consumers who have been harmed by, e.g., unfair, deceptive or abusive practices could be adversely affected if financial institutions are required to delete the data needed to identify victims.[32]

Given all this – and given that data retention has much less of an impact on privacy interests than data collection – we respectfully suggest that the Bureau should carefully reconsider the retention principle.

---

[32] For example, *In the Matter of Hello Digit LLC*, No, 2022-CFPB–0027, the CFPB required reimbursement to consumers who were adversely affected by an autosave withdrawal from January 2017 to August 2022. Not all of those victims could have been identified had Hello Digit been required to delete data for any consumer who terminated the service during that period of time.

C. Secondary Uses and Data Retention (Outline III-E-iii, iv)

We are in general agreement with the need to establish limitations on secondary use of consumer-authorized data and on the importance of differentiating between different types of secondary uses. We also think it may be useful to differentiate between third parties who receive data in order to deliver a product or service to consumers (third party data recipients) and third parties who are effectively authorized to act as conduits (i.e. data aggregators) for such data recipients/product or service providers. In this regard we offer the following thoughts.

Distinguishing Primary from Secondary Use. Innovations of all sorts depend on the ability of third party data recipients to learn from those data. Indeed, consumers' grants of data access to their financial data has in numerous circumstances created a virtuous circle in which third party data recipients both provide valuable services and use incoming data to further improve or expand upon their services in much the same way that data providers themselves may do as part of their own product development processes. At the same time, once a third party data recipient has obtained data it was authorized to obtain, the privacy risks associated with that third party itself mining those data for new insights seem minimal at most. (We address the issues posed by data sharing below.) Thus, to assure an environment that fosters innovation – and to avoid putting data recipients at a disadvantage relative to data holders – we urge that any limits on the secondary use of data by a third party data recipient be defined so as to permit the data recipient to collect and use, as a "primary use," data that is reasonably needed to *provide, improve, validate, or assess the efficacy and impact on users of a product or service the consumer has requested from the data recipient and to meet any legal obligations.*

Matching and Appending Data. Some third parties have found it necessary or at least highly useful to append to financial data that they have obtained with consumers' authorization other publicly or commercially available data about these consumers. For example, in its research on the efficacy of cash flow underwriting, FinReg Lab found that cash flow attributes and scores "frequently improved predictiveness in combination with traditional credit history."[33]

Sometimes matching can be done by bringing new datasets in house and merging those data with consumer-permissioned financial data. But for certain sources of data – most notably credit bureau data of the type just described -- any such matching must be done by the credit bureau given the restrictions on their disclosing PII. In these instances, the third party may need to share the data it has obtained with the credit bureau along with PII so that the credit

[33] FinReg Lab, "The Use of Cash-Flow Data In Underwriting Credit" at 28 (July 2019)

bureau can append its data and return an anonymized dataset. This is, indeed, the way in which the CFPB itself has built some of its data assets. We urge the Bureau to leave room in the rule it proposes for such data sharing at least so long as data shared by the third property remains its property and is not integrated into the database of a credit bureau.

Sharing Anonymized Data with Researchers and Policy Makers. At the CFPB's recent research conference, several papers were presented based on research that utilized anonymized transactional data that some financial service providers had obtained with consumers' authorization and had shared with researchers.[34] Such sharing poses minimal privacy or security risk (at least so long as account numbers are stripped from the data) and has demonstrable benefits in advancing understanding of consumer financial behavior and of how both privately provided products and services and public policies affect consumers' financial health. We therefore urge the Bureau to exclude such sharing from any secondary use restrictions. We recommend defining researchers in this context to include academics, non-profit organizations engaged in research, and the research arms of public agencies. Indeed, the Bureau may wish to go further and leave room for the development by a consortium of data aggregators and third parties of a combined database managed and maintained by a bona fide non-profit entity and that would be used solely for research purposes, including providing researchers access to anonymized data.

Sharing Data for Commercial Uses. In contrast to the use cases described above, we believe the Bureau should tightly limit the ability of an authorized third party to sell, license, or otherwise allow another commercial entity to use personally identifiable, consumer-permissioned data for use in cross-selling other products or services. Given the risk that consumers will scroll through disclosures at the point of authorizing data access, we do not believe that third parties should be permitted to engage in commercial sharing unless authorized by the consumer expressly and in close proximity to the time at which the third party proposes to share the data.

In making this recommendation we recognize, of course, that the Gramm-Leach-Bliley Act takes a different approach and allows data sharing with third parties unless a consumer "opts out" and thereby directs a financial institution not to share the consumer's data. But experience suggests that few consumers read the opt-out notices they receive and thus that the opt-in regime has failed to achieve meaningful consumer control of their data. Accordingly, we

---

[34] *E.g.* DeHaan *et al.*, "Buy Now Pay (Pain) Later," https://files.consumerfinance.gov/f/documents/cfpb_2022-research-conference_session-1_lourie_paper.pdf; DiMaggio *et al, "* Buy Now, Pay Later Credit: User Characteristics and Effects on Spending Patterns," https://www.hbs.edu/faculty/Pages/item.aspx?num=62913

believe a different approach is warranted under § 1033 even though that would mean disfavoring data secured from this channel relative to other forms of data.

D. Data Accuracy and Dispute Resolution (Outline III-E-3)

The data that third parties obtain from data providers is derived from systems of record that depend existentially on the accuracy of the balances and transactions for which they account and the ledgers they maintain for individual deposit or credit accounts. Safety and soundness regulations require financial institutions to maintain such systems to high levels of reliability and accuracy. Indeed, the existence of sound financial markets and systems rely—existentially—on the soundness of such systems. Thus, so long as data is not somehow corrupted in the process of moving from a system of record to a data portal – and the Outline separately proposes to require data providers to implement reasonable policies and procedures to ensure that the transmission of data does not introduce inaccuracies – it seems to us that the risk of inaccuracy is low.

At the same time, it is not clear to us what third parties can do to ensure the accuracy of the data they collect or even what they could do if a consumer were to dispute the accuracy of a particular item of information. Given all this, and given the costs that would be entailed if every third party data recipient —many of whom, including companies FHN has been proud to help nurture, are small start-ups with few if any employees –were required to implement policies and procedures to assure accuracy and to research and process consumer disputes regarding inaccuracies, we would urge the Bureau not to impose accuracy or dispute resolution requirements on such third parties.

Different considerations are implicated when, pursuant to a commercial relationship with data recipients, an aggregator or other third party takes "raw" data from a data provider and cleans, transforms, categorizes, organizes, or otherwise manipulates the data. These processes can, indeed, introduce inaccuracies if, for example, data is misclassified. And if the output from these processes is used in credit decisioning, the inaccuracies can cause material harm to consumers. However, we believe the Fair Consumer Reporting Act (FCRA) provides a satisfactory framework for consumer protection in this context.

The question of whether or under what circumstances the FCRA applies to consumer-permissioned data used in a credit decision has been hotly debated. It seems clear, however, that when an aggregator or other third party transmits consumer-permissioned data for use in underwriting it is "communicate[ng] information … bearing on a consumer's credit worthiness, credit standing, [or] credit capacity .. which is used or expected to be used … for the purpose of

serving as a factor in establishing the consumer's eligibility for credit."[35] Such a communication qualifies as a "consumer report" under the FCRA so long as the entity making the communication "regularly engages .. in the practice of assembling or evaluating credit information or other information on consumers for the purpose of furnishing consumer reports" and thus constitutes a "consumer reporting agency."[36] And, in our view, at least where the aggregator or other third party does something more than function as a pipe in merely transmitting raw data from a data provider to a creditor – where, for example, the aggregator or third party cleans or classifies data -- we believe that aggregator or third party is engaged in "assembling or evaluating credit information" and thus that the FCRA applies to its activities.

If this analysis is sound, it follows that those involved in assembling and communicating consumer-permissioned data for credit underwriting (or other permissible purposes under the FCRA) have a duty to take reasonable steps to assure maximum possible accuracy and that consumers have a right to see the data that is assembled and to dispute its accuracy.[37] Rather than attempting to create an entirely new regime for addressing accuracy issues, we urge the Bureau to issue an interpretive rule clarifying the applicability of FCRA in the circumstances described above. [38]

Outside of the credit context (and related contexts governed by the FCRA), aggregators can, of course, introduce inaccuracies in the way they clean, categorize, or otherwise manipulate data. We thus can see value in imposing on aggregators – as distinguished from third party data recipients – an obligation to maintain reasonable policies and procedures to ensure that their work does not introduce inaccuracy, including procedures related to addressing disputes submitted by consumers. If the Bureau were to proceed down that path, we would encourage the Bureau to seek to harmonize any obligations it imposes with those that the FCRA imposes in the credit context.

---

[35] 15 U.S.C. § 1681a(d)(1)(A)

[36] *Id.* § 1681a(f).

[37] *Id.* § 1681e(a)

[38] As defined in 15 U.S.C. § 1681i. For the consumer to dispute the information, a consumer would need to be able to see a copy of the "consumer report" on which the decision was based and which they are entitled to do under the FCRA following an adverse action. However, unlike traditional "credit reporting companies" that maintain data files on consumers for purposes of compiling and delivering consumer reports on demand, the aggregators do not maintain consumer files in the same way and thus arguably should not be required to provide "file disclosures" in the same way that traditional CRAs do as outlined in 15 U.S.C. § 1681g.

Conclusion

Almost twelve years have passed since Congress enacted § 1033 and directed the Burau to issue implementing rules and two years have passed since the Bureau took the first step in this direction with an Advance Notice of Proposed Rulemaking. The launch of the SBREFA process is an important step forward. We urge the Bureau to proceed expeditiously to issue a Notice of Proposed Rulemaking, even if that means deferring resolution of some issues or leaving some details to be worked out based on experience through the supervisory process which, given the absence of any private right of action, is likely to be the primary means through which § 1033 law evolves.