1350 Eye Street NW, Suite 350, Washington, DC 20005 | 202-768-8950 | fpf.org

December 21, 2023

Via Electronic Submission

Director Rohit Chopra
Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552

Re: Comments on the Required Rulemaking on Personal Financial Data Rights (Docket No. CFPB–2023–0052)

Dear Director Chopra,

On behalf of the Future of Privacy Forum (FPF), we are pleased to provide comments and recommendations to the Consumer Financial Protection Bureau (CFPB) regarding the Required Rulemaking on Personal Financial Data Rights.[1]

FPF is a global non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies.[2] FPF is focused on advancing responsible data practices and has deep expertise regarding privacy and data protection, particularly concerning the privacy implications of open banking. Our comment's recommendations reflect the belief that privacy is foundational to trust in and the uptake of open banking products and services. In addition to its traditional expertise, for open banking, FPF may offer a unique perspective as it hears from stakeholders across the open banking spectrum.

FPF applauds the central features of the NPRM. It importantly provides:

1. Customer control and benefits driving industry obligations and activities;
2. Privacy and security expectations for all industry players;
3. A needed role for industry standards within the regulatory framework; and
4. The phase out of screen scraping where consumers share online credentials with third party companies.

FPF offers the following comments and recommendations to support the CFPB's goals, under each subpart of the NPRM. Our main recommendations relate to:

1. Strengthening requirements for standard-setting bodies;
2. Supporting standards for data provider denials of access to the developer interface or requested information;
3. Developing consistency for privacy obligations of third parties;

[1] Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74796 (Oct. 31, 2023).
[2] The views expressed in this comment are those of FPF and do not necessarily reflect the views of FPF's supporters or Advisory Board.

4. Supporting an opt-in standard and use of de-identified data, while providing an approach for high-risk uses;
5. Clarifying certain definitions and compliance dates; and
6. Strengthening the phase-out of screen scraping as a poor privacy and security practice.

I. Subpart A - Recommendations Regarding Compliance Dates, Definitions, and Standard Setting

FPF offers the following comments related to Subpart A, relating to compliance dates, definitions, and standard setting.

A. Data provider's obligations should be tied to availability of developer interfaces pursuant to a qualified industry standard

Per the CFPB request regarding timelines in proposed Section 1033.121,[3] FPF recommends that the compliance clock be tied to availability of standard formats to transmit covered data via developer interfaces. This is the foundation of data sharing under the rule.

FPF supports the rule to require that the interface meet a qualified industry standard.[4] In order for the clock to start, the CFPB must have recognized the relevant standard-setting body, and that body must have issued the standard. The rule should provide reasonable compliance timeframes, after issuance of the standard, based on data provider attributes described in the rule.[5]

B. The Bureau should seek to harmonize key definitions from the 1033 rule and its Fair Credit Reporting Act rulemaking

The CFPB should seek to harmonize key definitions from the 1033 rule and its Fair Credit Reporting Act (FCRA) rulemaking. This could be accomplished by publishing the final rules close in time to each other, so they could benefit from input from each other's rulemaking process, with harmonized compliance dates if and where helpful. Examples include harmonizing definitions relating to aggregators, data brokers (or sales of data), and what activities make an entity a furnisher for purposes of the FCRA. At a minimum, in its Section 1033 rule, the CFPB should clarify that when a data provider gives a third party access to data via a developer interface, it is not furnishing data to a consumer reporting agency. Partly for this reason, and in response to the CFPB's request, FPF suggests renaming aggregators in this rule.

FPF understands that the CFPB is operating under at times competing public policy goals, to implement Section 1033 rules carefully and with minimal disruption, while also continuing to move the ball forward, recognizing that delay and uncertainty creates its own market

---

[3] Required Rulemaking on Personal Financial Data Rights, *supra* note 1, at 74806–07, 74815

[4] In response to the CFPB's question on NPRM page 76 about the viability of Section 1033.311(b)(2), related to widely used formats, FPF considers it could be eliminated if a qualified industry standard exists. In FPF's view, the best outcome is for industry to use a standard issued by a body recognized by the CFPB. All players will know what the standard is. The standard should also be high quality and have credibility based on how it is developed and recognized. If so, Section 1033.311(e)(1)(ii)(B) could probably also be eliminated, which has similar implementation challenges.

[5] FPF anticipates the Bureau will receive comments from the data provider community about reasonable implementation timelines.

disruptions. FPF appreciates the thoughtful work the CFPB has done to develop this rule to date, for the long-term benefit of consumers and the competitive marketplace.

C. FPF recommends the Bureau review the varying notices and choices that consumers receive to determine consumer impact and potential improvements that policymakers can make, including harmonizing requirements

The agency should review the varying notices that consumers receive, which increasingly provide a different set of choices and rights, to determine consumer impact and potential improvements that policymakers can make, including harmonizing requirements. Data providers and third parties may need to provide multiple notices to consumers due to the Section 1033 rule, Gramm-Leach Bliley Act (GLBA), and other laws and regulations, leading to confusion among consumers. The GLBA and its implementing regulation, Regulation P, require financial institutions (FIs) subject to the Bureau's jurisdiction to provide customers with privacy notices.[6] The proposed Section 1033 rule also contains a notice requirement, obliging authorized third parties to provide consumers with an authorization disclosure before obtaining covered data from a data provider.[7] Some of these entities may also need to make separate disclosures to comply with state data privacy laws.[8]

There is potential overlap between entities that qualify as FIs, authorized third parties, and organizations subject to state data privacy laws, potentially creating challenges that FPF flags for the Bureau's awareness. These entities may need to provide multiple, segregated notices, depending on their role within the open banking ecosystem.[9] As an example, data providers may also be an authorized third party as open banking becomes more reciprocal. These entities may need to provide different notices under the GLBA, Section 1033 notices, and state laws, each presenting their own unique rights and choices. In these circumstances, consumers would receive varying kinds and amounts of information depending on the applicable legal regime, resulting in different levels of transparency into data processing activities and potential confusion about individual rights.

The multiplicity of notices and choices may create significant compliance challenges for entities and confuse consumers. For example, organizations may need to tag data on the back-end with separate or overlapping codes. In light of these challenges, FPF therefore recommends that the Bureau seek to harmonize privacy rules' requirements.

---

[6] 12 C.F.R. § 1016.4(a) (2023).

[7] Required Rulemaking on Personal Financial Data Rights, *supra* note 1, at 74873 (Proposed Section 1033.411(a) states that this disclosure must also be "clear, conspicuous, and segregated from other material.").

[8] Cal. Civ. Code § 1798.130(a)(5) (2023) (The CPRA's GLBA carve-out is purpose-specific, meaning it exempts a financial institution from coverage to the extent it is engaged in GLBA-covered processing activities. Some of an FI's activities may not be a GLBA-covered processing activity, in which case the CPRA's notice requirements would apply.).

[9] Many of these laws require notices to be segregated or contained in a specific format, making it difficult for an entity to bundle notices and rights, even if they all relate to privacy and consumer rights or control.

D. Standard setting - FPF supports establishment of standard-setting bodies and recommends the CFPB require certain additional features

The CFPB asks for feedback regarding features of a standard-setting body and how it should be recognized.[10] FPF provides the following comments and recommendations on these questions.

FPF supports establishment of standard-setting bodies set forth in proposed Section 1033.141. Regulatory frameworks can integrate industry standards where appropriate for the maximum benefit of both. The regulation still provides the framework and principles of the substantive requirements, including parameters for the governance of the standard-setting bodies, and the industry standard provides detail based on technical or marketplace expertise, with the benefit of enhanced enforcement. If done well, it is a win-win and can also adapt more readily over time. FPF believes standard-setting will greatly benefit consumers in providing more efficient and consistent experiences, and will benefit industry for similar reasons. The road to open banking will be less bumpy and more certain.

FPF supports the attributes listed in proposed Section 1033.141 as well.[11] To best meet goals of Section 1033, and the important privacy and security needs of consumers, FPF offers the following additional features that should be required of a standard-setting body. These additional features are consistent with OMB Circular A-119,[12] which provides guidance to federal agencies on the value of adopting industry standards where appropriate (The Circular also provides criteria for how and when to accomplish adoption of industry standards, to be flexibly adapted to the particular rulemaking).

- Standards should generally be made public for public policy purposes and to encourage participation. Exceptions would be permitted where justified, such as if publicity could increase security risk.
- The standard-setting body should specify any criteria such as membership to use its standard. FPF considers membership to be preferable, so that parties can be engaged in ongoing developments. Costs should be addressed, perhaps with a sliding scale depending on party size or role.
- The body should require or at least encourage users to indicate in writing, available to consumers, other stakeholders and regulators, that they adhere to its standards. This will make participation and accountability clear, and support oversight and enforcement activities. A preferred option is for members to seek certification from the standard-setting body that they are compliant.[13]

---

[10] Required Rulemaking on Personal Financial Data Rights, *supra* note 1, at 74808.

[11] FPF suggests that §§ 1033.141(a)(3) and (6) could be combined, since both deal with publicly available and transparent due process features.

[12] Office of Mgmt. & Budget, Exec. Office of the President, OMB Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities (2016) https://www.nist.gov/system/files/revised_circular_a-119_as_of_01-22-2016.pdf (hereinafter "OMB Circular A-119").

[13] Related services that could be provided by a standard-setting body or other party are assessments, monitoring services, or certifications or seals of conformance. Development of such services is also consistent with OMB Circular A-119. The Circular includes several sections related to the importance of conformity assessments to promote compliance, and recommends use of industry assessments if they fulfill assessment purposes. If parties are representing adherence to a standard, there should be ways to show that they are actually compliant, independent from their own processes. Otherwise, the burden falls only on data providers, or regulators via exam processes. For example, these services could provide an avenue to take in complaints where non-compliance is observed.

- In case the body has difficulty establishing balance across all interested parties and at all levels—for instance because there may be fewer available participants from consumer groups, non-profits, or smaller entities so that they are obligated to participate in multiple places and become spread too thin—the CFPB can make the rule more flexible and achieve the same goals of wide participation. The rule could require the body to establish governance structures that will enable meaningful participation across all interested parties. An example is an advisory board that feeds into various committees. Consensus should also take into account the opinions of a certain sector. For instance, if all third parties or data providers oppose a direction, it should not be adopted.
- The standard-setting body should reach agreement with the Bureau about how it will engage with or report to the Bureau. For example, the body could send an annual report to the CFPB about its activities, such as about changes to its standard or governance.

The CFPB indicates it plans to issue guidance later about the substance of the standards.[14] FPF agrees that it is important to address substantive adherence to the rule, in addition to critical governance elements. Currently the NPRM only addresses governance elements, such as having open and balanced participation and due process characteristics. To forestall any argument the rule is limited to this role, FPF suggests the rule includes provision for substantive requirements. One option is to add a new number under proposed Section 1033.141(a) such as:

- Standards content: Policies or other documentation address the relevant portion of the regulation for which the body seeks CFPB recognition.

E. Standard setting - FPF supports CFPB recognition of standard-setting bodies and offers recommendations about the recognition process including timing

FPF supports the need for the Bureau to recognize a standards-setting body so that companies are incentivized to use standards it issues. To encourage standard-setting bodies to be set up, and develop governance, processes, and standards, it is important for the CFPB to provide information about its process. FPF recommends that the CFPB develop guidance for its recognition process (including appeals) and related timelines, and FAQs or equivalent documentation to industry about this process. Guidance and FAQs should account for feedback to the body, such as the areas of its submission that need improvement, and also its typical timeframes for feedback and recognition.

The CFPB asks about timing of its recognition process—whether it should occur before, after, or close in time to the body issuing standards—or if its timing should be flexible.[15] FPF considers timing should be flexible. Some bodies may want CFPB recognition in order to proceed. Others may first want to build up momentum and governance processes.

[14] Required Rulemaking on Personal Financial Data Rights, *supra* note 1, at 74808.
[15] *Id.*

II. Subpart B – Recommendations Related to Data Provider Obligations to Make Covered Data Available

A. FPF urges the agency to further specify the kinds of data that qualify as terms and conditions and rewards information

FPF recommends that the Bureau further specify the kinds of data that are terms and conditions (T&C) or rewards information. The proposed rule articulates several examples of T&C information that fall within the definition of covered data,[16] and the NPRM provides a definition of this data type.[17] FPF recommends that the agency specify the examples of T&C information that data providers must share with authorized third parties to those that are reasonably necessary to provide the consumer's requested product or service. Requiring data providers to share all of a contract's T&C information with authorized third parties could conflict with the proposed rule's data minimization requirements, since this kind of information is rarely used to enable today's open banking use cases. T&C information is not typically the data consumers wish to port. Instead, data providers could make this information available via a link.

The CFPB should clarify what counts as rewards information. The proposed rule indicates that rewards information can be covered data, including transaction and T&C information.[18] However, there are many different kinds of rewards information, making the extent to which rewards information qualifies as covered data unclear. The lack of industry agreement on the meaning of rewards information adds to this uncertainty. This rulemaking process is therefore an opportunity for the Bureau to help clarify what rewards information falls within the scope of the proposed rule's data sharing obligation.

III. Subpart C – Recommendations Related to Data Provider Interfaces and Responding to Requests

The proposed rule places obligations on data providers, as the trusted holders of consumer financial information, to develop and manage various open banking processes. Examples include establishing developer interfaces meeting performance criteria; providing covered data through the interface; denying interface or informational access to authorized third parties based on risk management and other criteria; and potentially performing some confirmations with consumers regarding authorization disclosures and revocations. The Bureau indicates that the proposed rule will not change consumers' rights to recoup financial transfer errors through their financial institution.[19]

---

[16] Required Rulemaking on Personal Financial Data Rights, *supra* note 1, at 74870 (proposed Section 1033.211(d) states that examples of T&C information include "the applicable fee schedule, any annual percentage rate or annual percentage yield, rewards program terms, whether a consumer has opted into overdraft coverage, and whether a consumer has entered into an arbitration agreement."); *Id.* (proposed Section 1033.221(a) states that covered data does not exit the scope of the proposed rule's data sharing obligation "merely because it is an input to, or an output of, an algorithm, risk score, or a predictor. For example, annual percentage rate and other pricing terms are sometimes determined by an internal algorithm or predictor but do not fall within this exception.").

[17] *Id.* at 74811 ("Terms and conditions generally refer to the contractual terms under which a data provider provides a covered consumer financial product or service.").

[18] *Id.* at 74870 (proposed Sections 1033.211(a) and (d) indicate that "rewards credits" and "rewards program terms" are examples of transaction information and T&C information respectively).

[19] Proposed Section 10333.331(b)(1) should also be amended to allow for authentication of data aggregators where they are in the data request flow.

FPF offers the following commentary and recommendations regarding data provider denials of access and information, as well as revocation mechanisms.

A. FPF supports the rule's encouragement of more consistent approaches and processes for data provider denials of interface access or information requests

FPF supports the ability of data providers to deny authorized third party requests for interface access or for information (hereinafter "data provider denials") based on appropriate security and risk management concerns.[20] Data providers are expected to protect consumer's data and accounts. Under the rule, however, FPF believes that data provider denials may not necessarily have consistent rationales, processes, or timelines, leading to potential disruptions or poor experiences. After exploring potential challenges, FPF offers some suggestions for consideration.

Under proposed Section 1033.321(a) and (b), data provider denials are not unreasonable if necessary to comply with Section 39 of the Federal Deposit Insurance Act or Section 501 of the Gramm-Leach Bliley Act,[21] and if the denial is specific and applied in a consistent and non-discriminatory manner.[22] As the CFPB points out, data providers have established risk management functions and processes and operate under third-party risk management guidance issued by prudential regulators including the Federal Reserve, OCC and FDIC. The guidance, which was updated in June 2023, is contained in OCC Bulletin 2023-17. The OCC Bulletin outlines a flexible and thorough approach for evaluating and responding to third party risks. Under the OCC Bulletin, "due diligence includes assessing the third party's ability to: perform the activity as expected, adhere to a banking organization's policies related to the activity, comply with all applicable laws and regulations, and conduct the activity in a safe and sound manner." Third party risks typically but not always relate to vendors operating under the financial institution's control; under Section 1033, few of the third parties will be bank vendors.

An initial question is which risks will be applied and how. If a data provider and a third party disagree over the sufficiency of the risk controls in place at the third party—that could itself be a bank—it is unclear how this conflict is resolved. We note that these are likely not solely back end disputes between the parties. The authorized third party has an independent relationship with the consumer, who has signed an authorization disclosure and is waiting for a requested product or service.

In addition to which risks are applied, there are timing questions about when data providers can request or receive evidence as to a third party's security and risk management practices. The first contact a data provider may have with a third party is when the third party makes a request to the developer interface with a signed authorization disclosure in hand (all the criteria needed to be an authorized third party). Data providers may deny these requests until the third party has

[20] Under proposed Section 1033.321, data providers may deny interface access requests based on permissible risk management concerns. This section is incorporated by reference for denials of information requests under proposed Section 1033.331(c)(1).
[21] Page 74820 of the NPRM indicates that "a denial would not be unreasonable if it is necessary to comply with safety and soundness requirements or data security requirements in Federal law."
[22] Requiring data providers to be specific about the reasons for their denials is valuable, as it enables the third party to correct deficiencies. Data providers, at least the large ones, tend to have sufficient resources to provide detailed denials. Similarly, data providers may issue denials that are internally consistent but not consistent across data providers. Proposed Section 1033.321(b)'s requirements relating to specificity, consistency, and non-discrimination are important but do not address all challenges relating to denials.

provided evidence that its practices are considered adequate to safeguard the covered data. A pre-vetting or registry process via a standard-setting body could help.

In this regard, FPF supports proposed Section 1033.321(c), which permits qualified industry standards to provide an indicia of reasonableness for denials related to data security or risk management. Alternatively, the rule could encourage the development of industry best practices that do not necessarily rise to the qualified industry standard level. Either model can address issues related to risk assessment methods, assessment timing, governance processes, and coverage for third parties and aggregators. In addition, to the extent data providers have concerns related to risks unique to them, they can raise those concerns as part of the communications with a third party in relation to its provision of evidence of adequate practices.

FPF also recommends the CFPB consider how to support progress from where the marketplace is now. The agency may want to include, in its preamble to the final rule, support for existing data flows that meet or substantially meet the rule's provisions, or language to address legacy data in some fashion. Data providers may otherwise deny access for data flows that are currently working between the parties under processes that are very similar to what is proposed under the rule (as long as existing contractual rights and responsibilities remain unchanged).

In sum, FPF wishes to underscore the centrality of the data provider denial process. Without data flows, open banking does not exist. The NPRM contains some consumer protection features that help minimize risks of unauthorized transfer, such as phasing out screen scraping.[23] This only makes the data provider denial processes even more important to be accomplished correctly. FPF recommends that the denial process be made clearer, as well as more consistent across providers, via industry efforts within the regulatory framework.

B. The agency should clarify when revocation mechanisms are likely to interfere with, prevent, or materially discourage consumers or authorized third parties' access to or use of covered data

The Bureau should provide examples regarding when revocation mechanisms are likely to interfere with, prevent, or materially discourage consumers or authorized third parties' access to or use of covered data. Under the proposed rule, data providers may create a "reasonable" mechanism for consumers to revoke a third party's authorization to access all of their covered data.[24] The proposed rule provides minimum requirements for a revocation mechanism to be

[23] Required Rulemaking on Personal Financial Data Rights, *supra* note 1, at 74801 (noting features of the proposed rule that are designed to minimize risks of unauthorized transactions and other errors. These include allowing data providers to share TANs, not allowing data providers to rely on credential- based screen scraping to satisfy their obligations under CFPA section 1033, clarifying that data providers can engage in reasonable risk management activities, and implementing authorization procedures for third parties that would require they commit to data limitations and compliance with the Gramm-Leach-Bliley Act (GLBA) Safeguards Framework.") (footnote omitted).

[24] Required Rulemaking on Personal Financial Data Rights, *supra* note 1, at 74872.

reasonable, which resemble other U.S. laws[25] and foreign rules'[26] language addressing manipulative design practices online. The design and default settings of online services may constitute unlawful manipulative design (also called deceptive design or "dark patterns") when they impair users' intentional decision-making. The NPRM also solicited feedback on deceptive design that occur when third parties seek opt-in consent for secondary uses.[27]

FPF recommends that the agency provide a list of examples of how deceptive design might manifest in the revocation mechanism context. Deceptively designed revocation mechanisms could hinder or prevent individuals from using open banking products or services. At the same time, data providers may find it challenging to distinguish between manipulative design and lawful persuasive practices. Articulating a non-exclusive list of examples of the sort of "dark patterns" that proposed rule prohibits could help reduce the likelihood of consumer harm arising from such practices and facilitate compliance. Emphasizing that the list is non-exhaustive would maintain the Bureau's flexibility to enforce against novel forms of manipulative design. In formulating these examples, the Bureau could draw from the Colorado Privacy Act (CPA) regulation[28], its own work,[29] and that of the Federal Trade Commission (FTC), which has a long history of analyzing and enforcing against design practices that obfuscate or subvert consumer privacy choices.[30] The agency should also consult these resources to develop requirements governing third party solicitation of opt-in consent for secondary uses, as dark patterns can occur in this context as well.[31]

---

[25] Required Rulemaking on Personal Financial Data Rights, *supra* note 1, at 74872 (To be reasonable, the "revocation method must, at a minimum, be unlikely to interfere with, prevent, or materially discourage consumers' access to or use of the data, including access to and use of the data by an authorized third party."); The Bureau's focus on "dark patterns" in the context of consent and the revocation thereof is consistent with the approaches seen in comprehensive state data privacy laws like the CPRA and Connecticut Data Privacy Act (CTDPA), which typically cabin their dark pattern proscriptions to consent flows.

[26] Jurisdictions outside the U.S. have also sought to address dark patterns that can occur when consumers provide and withdraw their consent for open banking products and services. *E.g.*, Eur. Comm'n, *Proposal for a Regulation on a framework For Financial Data Access*, COM/2023/360, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023PC0360, ("[The permission dashboard] should not be designed in a way that would encourage or unduly influence the customer to grant or withdraw permissions.").

[27] Required Rulemaking on Personal Financial Data Rights, *supra* note 1, at 74837 ("[T]he CFPB requests feedback on how opt-in mechanisms could be implemented to prevent third parties from using "dark patterns" or deceptive practices aimed at soliciting consumer consent.").

[28] Colo. Code Regs § § 904-3-7.09 (2023), https://coag.gov/app/uploads/2023/03/FINAL-CLEAN-2023.03.15-Official-CPA-Rules.pdf; Cal. Code Regs. tit. 11, § 7004(a)(1)–(5) (2020) (These examples could also incorporate the principles for obtaining consumer consent from the California Consumer Privacy Act regulations, including (i) easy to understand, (ii) symmetry in choice, (iii) avoid language or interactive elements that are confusing to the consumer, (iv) avoid choice architecture that impairs or interferes with the consumer's ability to make a choice,and (v) easy to execute.).

[29] CFPB, *CFPB Issues Guidance to Root Out Tactics Which Charge People Fees for Subscriptions They Don't Want*, (Jan. 19, 2023), https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-guidance-to-root-out-tactics-which-charge-people-fees-for-subscriptions-they-dont-want/.

[30] FTC, *Bringing Dark Patterns to Life*, (Sept. 15, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

[31] Felicity Slater, *The Future of Manipulative Design Regulation*, FPF (Jan. 19, 2023), https://fpf.org/blog/the-future-of-manipulative-design-regulation/ (noting that "manipulative design

IV. Subpart D – Recommendations Related to Authorized Third Parties

FPF offers the commentary and recommendations regarding authorized third parties, touching on the following areas:

- Additional examples of how to apply the reasonably necessary standard;
- Support for an opt-in standard and how to define high risk uses;
- Consistent implementation of collection, use and retention restrictions;
- Use of de-identified data;
- Clarifying the role and responsibilities of data aggregators; and
- Phasing out unsafe screen scraping practices, not just by data providers preventing them, but from third parties conducting these activities directly.

A. FPF recommends that the Bureau provide additional examples of how to apply the reasonably necessary standard

FPF supports the use of the "reasonably necessary" standard to limit how authorized third parties may use consumer data. It is an appropriate way to put guardrails around data uses that reflects modern privacy sensitivities while providing a standard that can be adapted to developing business models and innovation.

FPF recommends modifying proposed Section 1033.421(c) to state that product improvement is related to servicing the requested product. If an authorized third party finds that one or more consumers struggle with a product feature, and prefer another approach, the company should change the product consistent with consumer feedback. FPF accordingly suggests modifying proposed Section 1033.421(c)(3) as follows: "Servicing, processing, or improving the product or service the consumer requested." The final rule could describe and place limits on an authorized third party's ability to use covered data for product improvement purposes.[32] If consumers prefer a certain user experience flow, that can and should be deployed for similar flows. This approach reflects and is stricter than good business practices today.

B. The final rule should include an opt-in standard for secondary uses and articulate a list of high-risk use cases

FPF recommends that consumers be able to opt in to secondary uses for open banking.[33] Open banking is about consumer direction, consistent with opt-in consent. Without the ability to opt in, authorized third parties may conduct some contortions to make related secondary uses into a separate product/service. This could lead to awkward consumer experiences.

FPF appreciates potential concerns about an opt-in standard due to the potential for consumers to inadvertently or against their own interest opt in to a secondary use that may be a higher risk

---

elements can steer individuals into unwittingly disclosing personal information, incurring unwanted charges, or compulsively using services.").

[32] Companies sometimes use non-attributable consumer commentary, such as during call center conversations, like "I am very confused by this process, please change it!!" to sell changes to upper management. This may be similar to how agencies use consumer complaints to create positive action.

[33] FPF does not believe that opt-in consent should apply to the three specific activities listed in proposed Section 1033.421(a)(2), including targeted advertising, cross-selling, or data sales.

activity than the initial use. The difficulty in defining high-risk uses should not lead the CFPB to exclude all opt-in secondary uses. In FPF's view, opt-in consent is the correct principled approach. Opt-in consent is also considered a gold standard in privacy; many regimes including under the GLBA use an opt-out standard regarding restricted uses or sharing. Certain secondary uses, well explained to a consumer, may provide key consumer benefits and support a competitive market. To guard against high-risk uses, the CFPB could create a watch list of products that have generated considerable agency scrutiny and enforcement actions, like certain types of loans.[34] In this regard, the CFPB could seek input from companies that have performed risk assessments regarding product offerings. The rule or guidance could cross-reference to this list as prohibited secondary uses. While these uses are still legal offerings, they can still be teed up as a separate product, whether under open banking or otherwise.

In response to the CFPB's questions about how to implement an opt-in standard,[35] FPF considers that the authorization disclosure can be a permitted vehicle, and opt-in consent should be as clear and as segregated as initial consents.

C. FPF recommends that the rule allow industry standards to be developed regarding appropriate collection, use, and retention of covered data within the 1033 framework

FPF notes that the Section 1033 restrictions on authorized third parties regarding the collection, use and retention of consumer data is a new regulatory obligation in the financial sector. The NPRM directs authorized third parties, in proposed Section 1033.421(e), entitled Data Security, to apply to its systems for the collection, use and retention of covered data an information security program that follows rules issued under Section 501 of the GLBA or by the FTC in 16 CFR part 314 (whichever is applicable).[36] These rules generally relate to the security of data and security incidents or breaches. Neither regulations provide detailed guidance on how to apply privacy standards relating to appropriate collection, uses and retention of data as contemplated by Section 1033. Without further guidance, either via regulation or industry standards, there will likely be quite inconsistent applications of these regulatory obligations. If third parties interpret the rules differently, consumers will experience inconsistencies in the choices or products they are provided, or in back-end uses of data, often without transparency. These inconsistencies may also drive data provider denials, as described above, which can result in product disruptions or other poor consumer experiences.

Amidst this uncertainty, FPF recommends that the rule allow qualified industry standards, or encourage industry best practices, to be developed regarding appropriate collection, use, and retention of covered data within the Section 1033 framework. These standards or practices will minimize business friction and provide better, more consistent experiences, for the benefit of consumers.

D. The Bureau should exclude de-identified data from the proposed rule concerning third party collection, use and retention of consumer data

[34] On preamble pages 244–45, the CFPB describes concerns about harmful secondary uses and seeks input about how they could be defined and prohibited.
[35] Required Rulemaking on Personal Financial Data Rights, *supra* note 1, at 74836–37.
[36] *Id.* at 74871.

The Bureau should clarify that de-identified data is not subject to the proposed rule's third party obligations related to the collection, use, or retention of consumer data.[37] Doing so would encourage the further development of open banking products and services in a privacy-protective manner. Under proposed Section 1033.421(a), authorized third parties must limit their "collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service."[38] According to the NPRM, this provision would apply to the collection, use, and retention of de-identified data.[39]

The use of de-identified data is a central aspect of data processing for all industry sectors, including the financial sector. In open banking, an example is quality control and product and service improvements.[40] Many of de-identification's risks stem from re-identification, which typically occur when organizations fail to correctly apply appropriate standards or release de-identified data sets to researchers or publicly. These risks are far less significant for data limited to internal uses and subject to strict controls. We recognize the widespread evidence of re-identification attacks, but also note that these have all been attacks on data that did not meet basic standards for de-identification.

In light of these benefits, the CFPB has a crucial opportunity to set fair rules for consumers and businesses. This is another area ripe for qualified industry standards, particularly since there is not a de-identification standard defined today for the financial sector.[41] Many effective regulatory approaches exist in the U.S. and globally, and many companies have devoted considerable expertise and resources to develop internal standards based on these frameworks, adapted to the sensitivity of the data and uses. There are many kinds of de-identification methods, from blurring or suppressing data to more robust techniques such as differential privacy. All of these methods aim to preserve the utility of data while promoting privacy, but it is important to strike the right balance.[42] FPF recommends the CFPB allow the use of de-identified data. With regards to the de-identification standard, the CFPB could encourage the adaptation of an

---

[37] De-identification and anonymization are not the same. *E.g.*, Kelsey Finch, *A Visual Guide to Practical Data Deidentification*, FPF (Apr. 25, 2016), https://fpf.org/wp-content/uploads/2017/06/FPF_Visual-Guide-to-Practical-Data-DeID.pdf (describing anonymized data as when "[d]irect and indirect identifiers have been removed or manipulated together with mathematical and technical guarantees to prevent re-identification.").

[38] Required Rulemaking on Personal Financial Data Rights, *supra* note 1, at 74873.

[39] *Id.* at 74836–37. (The CFPB seeks comments about its restrictions on use of de-identified data and what de-identification standard the rule should provide.).

[40] *See e.g.*, Stripe Privacy Center, https://stripe.com/en-lt/legal/privacy-center ("When Stripe communicates the results of its product performance analytics to Business Users or for advertising purposes, it does so only in aggregated or de-identified form that does not permit third-parties outside of Stripe to associate that data with any particular End Customers.").

[41] Finch, *supra* note 37 (There is no sole definition for de-identified data, with jurisdictions and organizations advancing different descriptions. The FPF infographic, which reflects consultations with experts and a review of how jurisdictions approach this concept, defines de-identification as when "[d]irect and known indirect identifiers have been removed or manipulated to break the linkage to real world identifiers."); *Protecting Consumer Privacy In An Era of Rapid Change*, FTC, 21 (Mar. 2012); *E.g.*, Va. Code Ann. § 59.1-575, (defining de-identified data as "data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person.").

[42] Daniel Berrick, *Comment on OSTP RFI Response: Privacy-Enhancing Technologies, Doc. No. 2022-12432*, (July 8, 2022) https://fpf.org/wp-content/uploads/2022/07/Future-of-Privacy-Forum-RFI-Response-Privacy-Enhancing-Technologies.pdf, ("For example, differential privacy may underestimate bias when the size of a dataset changes. In other circumstances, de-identification methods may not provide a sufficient level of privacy while retaining the underlying utility of data.") (footnote omitted).

existing de-identification regulation related to other sensitive data, or the development of industry standards as best practices or via a standards-setting body under the Section 1033 rule.[43] By doing so, the CFPB could enable the development of better products, services, and experiences for consumers, supported by strong consumer protections, while fostering needed consistency within industry.

E. The rule should encourage data aggregators to take on additional roles and obligations to support open banking and consumer experiences, and the Bureau should specify when data aggregators become authorized third parties

The agency should amend the proposed rule to enable aggregators to take on additional obligations. Open banking should allow the convenient and safe flow of information between parties at consumers' direction. In the short term, intermediaries can help enable data sharing between different parties that may have limited experience facilitating consumers' decisions to share data from their financial accounts with their financial services providers. Some of these issues will take some time to resolve, especially where there are potentially thousands of data providers and authorized third parties. Here, intermediaries with sufficient knowledge could help diminish friction and disruption.

Recognizing that authorized third parties have accountability, the rule should allow aggregators and authorized third parties to negotiate the ability for aggregators to take on additional obligations. Examples include responsibility for interfacing with consumers on the front end, such as via the authorization disclosure,[44] or navigating risk management with data providers on the back end, where they can bundle approaches of several authorized third parties. This should generate consumer and compliance benefits too. If the aggregator supports multiple third parties, the aggregator may be able to provide better consumer experiences, and perform stronger compliance activities, than each third party can individually.

FPF suspects and applauds that, with the Section 1033 rulemaking's direction, many aggregators will explore other ways to add value to consumers and open banking beyond a pass-through function. As an example, they can assist data providers and authorized third parties with data format needs and data minimization, which is an important privacy goal to minimize the amount of data requested and transferred. Under the NPRM, authorized third parties set what data they need for their product—data providers can only confirm these requests with consumers—so that there may be a gap if the data is potentially excessive and does not fit within the developer interface standard formats.

---

[43] As examples, qualified industry standards could require third parties to adopt de-identification standards, and appropriate analytics techniques, that mitigate the risk of re-identification to within a reasonable degree. Most legal approaches to de-identification standards emphasize having strong internal technical, administrative, and contractual controls, and mitigating risk to within a reasonable degree; FTC, *supra* note 42, at 21; The EU's General Data Protection Regulation (GDPR) also contains a reasonableness standard in assessing whether personal data is anonymized under the Regulation (i.e., in considering whether a person is identifiable, Recital 26 indicates that organizations should consider "all means reasonably likely to be used . . . .").

[44] Required Rulemaking on Personal Financial Data Rights, *supra* note 1, at 74841 (See this part of the NPRM for a discussion of accountability of third parties and aggregators, where the CFPB preliminarily places accountability on third parties. As the CFPB points out, the consumer will have expectations based on who their relationship is with. If with the aggregator, the parties should be able to negotiate accountability consistent with consumer relationships and expectations.).

In addition, FPF recommends that the rule place additional obligations on aggregators (and authorized third parties), including prohibiting them from reverse engineering data providers' proprietary algorithms and information. FPF supports supervision of aggregators that are larger participants per the CFPB's rulemaking on this topic.

Finally, the CFPB should clarify the circumstances in which data aggregators become authorized third parties. Clarifications could be provided in the definition or by examples. As part of this clarification, especially where an authorized third party is also interacting with a consumer, the rule should specify the obligations of each party, and whether it is on a per consumer or per application basis. For instance, if the aggregator is servicing a consumer with whom it has worked with before, but this time for a new third party, the rule should be clear whether all obligations need to be met anew.

F. FPF recommends that the final rule directly prohibit third parties from engaging in screen scraping

FPF recommends that the final rule directly prohibit third parties and aggregators from engaging in screen scraping for covered data. In light of the various risks and harms posed by screen scraping to consumers and businesses, FPF suggested that the Bureau discourage this practice in its comments on the SBREFA outline.[45]

The proposed rule prohibits data providers from granting third parties access to the data provider's developer interface using a consumers' credentials.[46] The NPRM elaborates on this provision, stating that data providers cannot permit screen scraping of the consumer portal once they establish a compliant developer interface.[47] FPF supports these provisions. As an added incentive to encourage parties to include additional data than covered data, the rule could enable data providers to prohibit screen scraping for all data it provides via the developer interface.

The final rule should similarly place prohibitions against screen scraping on third parties and aggregators directly. Otherwise, the rule is solely reliant on data providers to identify and prevent the activity. Screen scraping also creates risk management challenges for data providers.[48] Given the risks that screen scraping poses to consumers—including among others the over-collection of data, increased data inaccuracy, and fraud—the screen scraping prohibition should be placed directly on the parties performing this activity.

FPF understands that, while the proposed rule will shift open banking in the U.S. towards a non-credential-based system, screen scraping could continue during the staggered regulatory compliance dates. The proposed rule reflects the need for these grace periods, as smaller

---

[45] Zoe Strickland and Daniel Berrick, *Future of Privacy Forum comments on the CFPB's Outline of Proposals and Alternatives under Consideration related to its Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights*, 2 (Jan. 2023), https://fpf.org/wp-content/uploads/2023/01/FPFs-Comment-on-the-CFPB-Outline-of-Proposals-and-Alternatives-FINAL.pdf,.

[46] Required Rulemaking on Personal Financial Data Rights, *supra* note 1, at 74871.

[47] *Id.* at 74813 ("In particular, certain provisions[, including Section 1033.31,] would ensure that data providers make covered data available to third parties through a developer interface rather than through the screen scraping of a consumer interface.").

[48] *See e.g.*, Fed. Rsrv. Sys., FDIC, and OCC, *Interagency Guidance on Third-Party Relationships: Risk Management* (June 6, 2023), https://occ.gov/news-issuances/news-releases/2023/nr-ia-2023-53a.pdf.

organizations may find it challenging to quickly implement a non-credential-based system.[49] However, the proposed rule should directly prohibit third parties and aggregators from screen scraping following this period. The practice of consumer sharing of sensitive credentials should be phased out and eliminated for all parties.

V. Conclusion

FPF appreciates the CFPB's efforts to provide consumers with robust privacy, security and other protections in the open banking ecosystem, and to provide companies with appropriate rules and greater clarity about their obligations under the proposed rule. FPF is thankful for the opportunity to comment on these issues.

We welcome further opportunities to provide resources or information to assist in this important effort. If you have any questions regarding these comments and recommendations, please contact Zoe Strickland (zstrickland@fpf.org) and Daniel Berrick (dberrick@fpf.org) (cc: info@fpf.org).

Sincerely,

Zoe Strickland
Senior Fellow

Daniel Berrick
Policy Counsel

[49] Required Rulemaking on Personal Financial Data Rights, supra note 1, at 74869 ("A data provider must comply with . . . §1033.301 beginning on: (c) [Approximately two and a half years after the date of publication of the final rule in the *Federal Register*], for depository institutions that hold at least $850 million in total assets but less than $50 billion in total assets.").