American Bankers Association

Ryan T. Miller
Vice President & Senior Counsel
Innovation Policy
(202) 663-7675
rmiller@aba.com

December 29, 2023

The Honorable Rohit Chopra
Director
Consumer Financial Protection Bureau
1700 G St. NW
Washington, DC 20552

Via electronic mail: 2023-NPRM-Data-Rights@cfpb.gov

Re: Docket No. CFPB-2023-0052; Response to Request for Comment on Proposed Rule for Personal Financial Data Rights [RIN 3170-AA78]

Dear Director Chopra,

The American Bankers Association (ABA)[1] appreciates the opportunity to comment on the Consumer Financial Protection Bureau's (CFPB or Bureau) Proposed Rule on Personal Financial Data Rights, which implements Section 1033 of the Dodd-Frank Act[2] (NPRM). The NPRM is an ambitious yet thoughtful effort to balance numerous interests, such as consumer demand, prudential oversight, innovation, privacy protection, emerging markets, and security protocols. While some components may be functional, others may appear reasonable in the abstract but will break down in practical application. ABA urges the CFPB to incorporate feedback from stakeholders to develop a final rule that fulfills the promise of the consumer-permissioned data sharing ecosystem.

Given the complexity of the rule, the condensed comment period did not afford stakeholders adequate time to assess an entirely new regulatory framework with tendrils into a myriad of operational and control functions. The Bureau should have designated additional time to submit comments, as multiple entities requested. As such, ABA may supplement these comments with information it would have provided had the Bureau established a deadline commensurate with the NPRM's impact.

Recommendations to the Bureau

As stated throughout the CFPB's rulemaking efforts with regard to Section 1033 over the past several years, ABA supports consumers' right to access their financial information securely, transparently, and subject to their control. At the same time, it is essential that all participants in the data sharing ecosystem are held to the same high standards as banks in areas such as keeping consumers informed, resolving disputes, and so on. We appreciate the CFPB's efforts to preserve

[1] *The American Bankers Association is the voice of the nation's $23.4 trillion banking industry, which is composed of small, regional and large banks that together employ approximately 2.1 million people, safeguard $18.6 trillion in deposits and extend $12.3 trillion in loans.*

[2] *See* Consumer Financial Protection Bureau, Required Rulemaking on Personal Financial Data Rights, Proposed Rule and Request for Public Comment, https://www.federalregister.gov/documents/2023/10/31/2023-23576/required-rulemaking-on-personal-financial-data-rights.

the best parts of the market-led data sharing ecosystem while seeking to implement guardrails to protect consumers and market participants.

This letter will focus on delivering actionable guidance on the ways the Bureau can improve the effectiveness of the regulation.

I. The CFPB must create a final rule that comports with the bounds of authority delegated to it by Section 1033 of the Dodd-Frank Act[3] [page 3].

- The final rule must not prohibit data providers from assessing fees. Such a prohibition is not supported by law.
- Covered data fields pertaining to "authorized but not yet settled" transactions, "upcoming bill information," and "information to initiate payment to or from a Regulation E account" exceed the confines of the statutory text.

II. The CFPB must take a more active role in managing the data sharing ecosystem it is creating, while affording data providers flexibility to manage risk and prevent fraud [page 5].

- The CFPB must make clear that data providers are not responsible for ensuring third parties and data aggregators are complying with the final rule.
- The final rule should expressly prohibit third parties and data aggregators from engaging in screen scraping of any portal (including the consumer interface, developer interface, or regular online banking account) to access any data (covered or otherwise) that is available through a developer interface.
- There should be a clear and unambiguous basis to supervise data aggregators as a separate class since they are unique entities which, at the time of the NPRM, play a major role in the ecosystem.
- The CFPB must ensure a baseline of compliance with the final rule from nonbanks operating in the ecosystem.
- The final rule should encompass the full spectrum of risk management concerns that banks face, with a wider range of scenarios in which data providers may deny access to the developer interface.
- The final rule should encourage the use of Data Access Agreements and provide flexibility to combat fraud.

III. The CFPB must not mandate that Section 1033 be used as a vehicle to initiate payments to and from a Regulation E account [page 10].

IV. The CFPB must permit recoupment of costs as a matter of public policy [page 11].

[3] *See* 12 U.S.C. 5533.

V. In the final rule, the CFPB must clarify that data providers making information available pursuant to Section 1033 are deemed not to be furnishers under the Fair Credit Reporting Act [page 12].

VI. The CFPB should revise several sections of the regulatory text to avoid confusion or otherwise ensure the practical operationalization of the rule [page 13].

- If the CFPB believes that the Financial Data Exchange specification would be deemed to satisfy the standardized format requirement in the absence of a qualified industry standard, it should say so explicitly.
- The CFPB should include language to the effect that data providers are only required to make available covered data that they own or generate independently.
- Several fields of proposed covered data should be excluded because they create confusion or are impractical to operationalize.
- The CFPB should revisit its narrow construction of the statutory exceptions.
- Several metrics or operational targets applied to data providers are overly prescriptive or overly reliant on qualified industry standards and should be replaced with a requirement for the data provider to "act reasonably."
- The CFPB must provide additional detail around its concept of the consumer interface, especially given its role in determining eligibility for the exception.
- The CFPB should clarify its privacy expectations by providing examples of "brief description[s] of the product or service" (including developing its concept of a "stand-alone product" as referenced in footnote 130 of the preamble).
- Similarly, the CFPB should provide additional context around data use prohibitions as many third parties are not held to bank-like standards for the use and sharing of consumer personal information.
- Due to lack of meaningful consumer choice, any treatment of the data by data aggregators other than transmitting or for the uses laid out in 1033.421(c) should be prohibited.
- The CFPB must expound upon the status of data already in the ecosystem.
- The triggering event for the compliance dates should be the designation of a specification that is deemed to satisfy the standardized formats of a developer interface, not publication of the final rule in the Federal Register.
- The CFPB should create compliance dates for all participants, and the earliest such date should be 2 years after the relevant condition precedent.
- ABA provides a list of other recommendations for the CFPB to consider.

This letter is organized around these recommendations, which ABA urges the Bureau to implement in its Section 1033 final rule.

I. The CFPB must create a final rule that comports with the bounds of authority delegated to it by Section 1033 of the Dodd-Frank Act.

ABA is concerned that several aspects of the NPRM appear to exceed the legal authority of the statute. This section flags those provisions of the regulatory text that should be struck from the

final rule due to their ultra vires nature. These areas also have strong policy arguments against their inclusion, which are addressed in *Sections III, IV and VI*.

A. Fee Prohibition

The first example in the NPRM that is unsupported by law is the prohibition on fees ("[a] data provider must not impose any fees or charges on a consumer or an authorized third party in connection with: (1)…[e]stablishing or maintaining the interfaces required by paragraph (a) of this section; or (2)…[r]eceiving requests or making available covered data in response to requests as required by this part").[4] Importantly, the statute is completely silent on the question of fees. If Congress had intended for information under Section 1033 to be made without the ability to charge a reasonable fee, it would have said so expressly.

B. Covered Data

Second, several data fields in the NPRM go well beyond the limitations imposed by the statute. In pertinent part, 12 U.S.C. 5533 states:

> Subject to rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person **concerning the consumer financial product or service that the consumer obtained** from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data. The information shall be made available in an electronic form usable by consumers [**emphasis added**].[5]

The Bureau should note the use of the past tense ("obtained"). Limiting the covered data fields to those that have already occurred is not just a best practice, it is firmly ensconced in the authority conferred by the statute. Any data field that is not retrospective is therefore out of scope. This includes "information concerning authorized but not yet settled debit card transactions"[6] (because they have not yet finalized and are subject to a reconciliation process, and ergo have not been obtained) and upcoming bill information (as these are future state and have not yet been obtained).[7]

Critically, another covered data field that exceeds the Bureau's legal authority is the category "information to initiate payment to or from a Regulation E account."[8] Section 1033 was created as a way for consumers to "access information," not mandate specific functionality. The statute does not create an obligation to enable payment transactions initiated by third parties. Thus, this data field exceeds the powers delegated by Congress and should be struck. This concept is further discussed in *Section III*.

[4] *See* NPRM, *supra* note 2 at 1033.301(c).
[5] U.S.C. 5533(a).
[6] *See* NPRM, supra note 2 at 1033.201(b).
[7] Id. at 1033.211(b) and 1033.211(e).
[8] Id. at 1033.211(c).

The Bureau must operate within the constraints of the law and strike these categories in the final rule.[9] If there is a viable business case for providing data to enable functionality that goes beyond what is required by law, the ecosystem will move in that direction after implementing appropriate risk mitigants. However, that is not for the CFPB to decide.

II. The CFPB must take a more active role in managing the data sharing ecosystem it is creating, while affording data providers flexibility to manage risk and prevent fraud.

As the data sharing ecosystem matures, the uneven degree of oversight conducted on the various participants poses greater challenges. Banks are subject to a host of laws and regulations and undergo rigorous examinations by multiple agencies. This is for good reason—to protect consumers and ensure the safety and soundness of the financial system. Yet many newer types of financial services companies, such as fintechs, are comparatively unregulated or underregulated. Data aggregators[10] are a type of fintech that enjoyed exponential growth due to filling a need for intermediaries between other fintechs and traditional financial institutions.

In a June 2023 blog post, the Director discussed "Laying the foundation for open banking in the United States."[11] The post discussed the role of standard-setting organizations in the ecosystem. While industry participants have and will continue to play a critical role in developing the data sharing ecosystem, as the architect of the NPRM the CFPB must clearly and materially address its own role and responsibilities. As proposed, far too many portions of the NPRM are reliant on data providers or standard-setting bodies.

A. Data Providers

While data providers being empowered to authenticate consumers and to confirm the scope of a third party's authorization are beneficial and will help to mitigate fraud risk,[12] there are other responsibilities that the CFPB appears to expect data providers to perform that are less positive. For instance, data providers appear to have an obligation to prevent third parties from engaging in screen scraping and to confirm third parties have followed authorization procedures. Despite the CFPB's claim that it "does not believe primary enforcement responsibility for ensuring third parties are acting on behalf of consumers should reside with data providers,"[13] there is no other

[9] In addition to the fee prohibition and the data fields, we observe "data providers" as used in the NPRM means a financial institution as defined by Regulation E, a card issuer as defined by Regulation Z, and any other person that controls or possesses information concerning a covered consumer financial product or service the consumer obtained from that person (1033.111(c)). However, the Dodd-Frank Act placed certain limitations on the Bureau's jurisdiction. Accordingly, the final rule should clearly reflect this by expressly carving out any relevant limitations on the Bureau's authority under 12 U.S.C. 5517, such as entities regulated by the Securities and Exchange Commission (SEC). This will help avoid confusion in the marketplace among consumers and third parties seeking access to information.

[10] To clarify, we are referring to data aggregators operating within the consumer-permissioned financial data ecosystem, not the broader concept of data brokers or other types of aggregators.

[11] Rohit Chopra, "Laying the foundation for open banking in the United States," https://www.consumerfinance.gov/about-us/blog/laying-the-foundation-for-open-banking-in-the-united-states/.

[12] *See* NPRM, *supra* note 2 1033.331(b)(1)(i) and 1033.331(b)(2).

[13] Id. at preamble.

way to read some of the NPRM's regulatory text. In the final rule, the CFPB must clarify that data providers are not responsible for ensuring that third parties and data aggregators are in compliance.

Although the preamble to the NPRM acknowledges that screen scraping continues to present risks to consumers, the proposed regulatory text affords consumers and data providers no explicit protection from this practice. Indeed, the NPRM states only that "[a] data provider must not allow a third party to access the data provider's developer interface by using any credentials that a consumer uses to access the consumer interface."[14] Just as critically, there is no discussion of the third party attempting to access the consumer interface or online banking portal. The final rule should expressly prohibit third parties and data aggregators from engaging in screen scraping of any portal (including the consumer interface, developer interface, or regular online banking account) to access any data (covered or otherwise) that is available through a developer interface. Further, the CFPB should explicitly recognize the ongoing right of data providers to block any third party or data aggregator that attempts to flout this provision.

In addition, data providers appear to have the onus to "[c]onfirm when the third party has followed the authorization procedures in § 1033.401."[15] It is not immediately clear how this is to be done effectively at scale or how to verify small fintechs are meeting these requirements when they operate as data providers. It is very likely to lead to inconsistent and unpredictable results.

B. Data Aggregators

Data aggregators are not sufficiently supervised as a separate class, and the CFPB should use this rulemaking and its other statutory powers to develop a more comprehensive supervisory program for them. To that end, ABA reiterates its request that the CFPB pursue a larger participant rulemaking to directly supervise data aggregators.

ABA has previously petitioned the CFPB to commence larger participant rulemaking under 12 C.F.R. Part 1090 to directly supervise data aggregators.[16] This call was reiterated in ABA's response to the Bureau's Small Business Regulatory Enforcement Fairness Act (SBREFA) Outline.[17] The Director subsequently informed the petitioners that the CFPB declined to pursue the rulemaking, but noted that data aggregators were currently subject to supervision through existing authorities such as 12 C.F.R. 1091 (based on risk determination) and as larger participants in the consumer reporting market. The preamble to the NPRM alludes to some data aggregators being "regulated as…consumer reporting agenc[ies] under the FCRA [Fair Credit Reporting Act]."[18] This approach has its own problems, which will be addressed below in *Section V*. As will be discussed, the Fair Credit Reporting Act (FCRA) and the consumer

[14] Id. at 1033.311(d)(1).
[15] Id. at 1033.331(b).
[16] *See* American Bankers Association, et al., Joint Trades' Petition for Rulemaking Defining Larger Participants of the Aggregation Services Market (Aug. 2, 2022), https://www.regulations.gov/document/CFPB-2022-0053-0001.
[17] *See* American Bankers Association, Response to Outline of Proposals and Alternatives Under Consideration for Required Rulemaking on Personal Financial Data Rights, https://www.aba.com/advocacy/policy-analysis/letter-to-cfpb-on-data-sharing-rules.
[18] *See* NPRM, *supra* note 2 at preamble.

reporting market should not be entangled with consumer-permissioned data sharing under the Section 1033 final rule.

The NPRM defines a data aggregator as "an entity that is retained by and provides services to the authorized third party to enable access to covered data"—in other words, a service provider.[19] This is a stripped-down version of what a data aggregator is today, but it may signal the CFPB's approach since the Bureau enjoys supervisory authority over certain service providers as well.[20] It is also probable the Bureau is seeking to capture data aggregator activity in its proposed expansion of the definition of "financial product and service" under 12 C.F.R. 1001.2(b).[21] The amendment is characterized as a clarification, not a substantive change. Regardless, it should go farther than it does. If the intent is to capture data aggregators, it should do so directly. There should be a clear and unambiguous basis to supervise data aggregators as a separate class since they are unique entities which, at the time of the NPRM, play a major role in the ecosystem.

Indeed, the presence of data aggregators in the NPRM is very sparse. Where data aggregators are addressed explicitly or implicitly, they are often treated as just another third party.[22] For example, when retained to provide services to third parties, it is third parties that maintain the compliance risk.[23] This is despite the fact that data aggregators often possess far greater bargaining power, which will allow them to dictate terms. Accordingly, it is crucial that text in the final rule require that data aggregators are "jointly and severally liable" for issues that occur at the third party to which it is providing services (further necessary because there are legitimate questions of whether the third party is solvent or sufficiently insured to pay for harm it may cause). Similarly, the "flowdown terms" provision should be strengthened to specifically call out fourth and fifth parties.[24] These changes will incentivize all entities to be meticulous when pursuing contractual business relationships.

Further, data aggregators as a separate class should be expressly required to comply with the security requirements of the Gramm-Leach-Bliley Act (GLBA) to pass/receive consumer data through safe and secure channels. Directly addressing data aggregator risks is a better approach for everyone, including the CFPB's own examiners.

C. Fintechs

While there is no universal definition, fintechs can be understood as nontraditional financial institutions that use technology to deliver novel products and services to customers. These are distinct from traditional depositories such as banks and credit unions because they do not have a

[19] Id. at 1033.131.
[20] *See* 12 U.S.C. 5516(e).
[21] Providing financial data processing products or services by any technological means, including processing, storing, aggregating, or transmitting financial or banking data, alone or in connection with another product or service, where the financial data processing is not offered or provided by a person who, by operation of 12 U.S.C. 5481(15)(A)(vii)(I) or (II), is not a covered person. (c) [Reserved]. *See* NPRM, *supra* note 2 at 1001.2.
[22] One of the areas the NPRM does require action by the data aggregators is a disclosure to consumers, either directly or via a third party. *See* id. at 1033.431(c). This is unnecessary and the cavalcade of disclosures is likely to create fatigue among consumers—hence, they should just be integrated into one stream.
[23] Id. at 1033.431(a).
[24] Id. at 1033.421(f).

prudential regulator that has ongoing supervisory authority over them. Rather, they are subject to the enforcement powers of the Federal Trade Commission. Because many fintechs are small, most will likely not be eligible for supervision by the CFPB.

An exception is the 17 or so general-use digital consumer payments applications that are the subject of the ongoing larger participant rulemaking the CFPB is pursuing.[25] ABA is commenting on this rulemaking separately. However, on the limited subject of its applicability to the NPRM, ABA observes that bringing at least some fintechs under CFPB supervision affords a necessary regulatory lever to ensure compliance. However, it does not cover the entire ecosystem and only accentuates the supervisory gap for the vast majority of fintechs.

Moreover, ABA members have expressed significant concern that, absent an effective supervisory regime, some ecosystem participants may exploit the lack of oversight to reverse engineer the aggregated data they have compiled to learn the business practices of data providers and offer competing products without the same degree of consumer protection as do banks. This would violate the spirit of Section 1033.221(a) and be anti-competitive; accordingly, the Bureau must take appropriate steps to forestall it.

There must be some mechanism in place to ensure a baseline of compliance with the final rule from nonbanks operating in the ecosystem. The Bureau has a basis to oversee data aggregators and the largest fintechs, which we support. In addition, there are policies the CFPB can adopt to protect consumers and the broader ecosystem—namely, by allowing data providers the flexibility to manage risk and prevent fraud.

D. Risk Management

It would be impossible to overstate the importance of risk management to bank operations. This is a fundamental expectation of the prudential agencies responsible for preserving the safety and soundness of the financial system of which ABA members are the keystone. Banking regulators have a long history of communicating high expectations in the ways banks identify, assess, and mitigate their own risks. This is very much a priority for ABA, and we appreciate the Bureau incorporating risk management principles into the NPRM.

The NPRM recognized two authorities for risk management that can be cited as reasonable bases to deny access to the developer interface, namely section 39 of the Federal Deposit Insurance Act, 12 U.S.C. 1831p-1 or section 501 of the GLBA.[26] While these are indeed valid risk management concerns, by themselves they do not go nearly far enough to account for all the risks that banks must address in order to comply with interagency guidance.[27] It is unclear

[25] *See* Consumer Financial Protection Bureau, Defining Larger Participants of a Market for General-Use Digital Consumer Payment Applications, Proposed Rule and Request for Public Comment, https://www.federalregister.gov/documents/2023/11/17/2023-24978/defining-larger-participants-of-a-market-for-general-use-digital-consumer-payment-applications.
[26] *See* NPRM, supra note 2 at 1033.321.
[27] *See* Interagency Guidance on Third-Party Relationships: Risk Management, https://www.federalregister.gov/documents/2023/06/09/2023-12340/interagency-guidance-on-third-party-relationships-risk-management.

whether these are intended as examples or if they were meant to be exhaustive. The final rule should be updated to encompass the full spectrum of risk management concerns that banks face, with a wider range of scenarios in which denial would be permissible under the rule.

For example, fraud is a constant source of worry for ABA members. As mentioned earlier, it is helpful that data providers are responsible for authenticating the consumer and are permitted to confirm the scope of the third party's authorization,[28] but there is always risk that there has been an identity compromise. Further, even if it is the actual consumer, there is always the possibility that the third party itself is a bad actor.

It is critical that data providers have the flexibility to manage these risks and prevent fraud. This is mandatory because the prudential banking regulators will hold banks accountable regardless of whether the CFPB recognizes the need or not. Depending on the structure of the final rule, the CFPB could create a situation in which the bank will have to choose whether to violate its commitment to financial stability or its compliance with Section 1033. This is an area in which no one wins—especially consumers, who might suffer harm if their information is released to questionable entities.

The final rule should continue to be framed such that data providers have the right, but not the affirmative obligation, to block access for risk management concerns under Section 1033, thereby allowing them to comply with prudential agency guidance. This right should continue to be in effect, even after the initial connection. Moreover, the CFPB must expand on its expectations for logging and monitoring these risks, which may influence how vendors build compliance solutions—which will aid small banks (there is a precedent for this with NY DFS cybersecurity requirements).

Further, banks should be under no obligation to engage with a blocked third party or inform them of the reason for the denial.[29] Some of these entities may be on sanctioned lists and it may be a violation of law to communicate with them; in any event, it is certainly not prudent in many cases.

A component of risk management that is not reflected in the NPRM is the Data Access Agreement (DAA). Data providers should retain the right to enter into DAAs to negotiate certain provisions, such as indemnification, insurance, and other commercial terms. The prescriptive response timeframes in the NPRM are not realistic with respect to the time it takes to negotiate a DAA. Accordingly, they should be withdrawn in favor of a principles-based "act reasonably" standard as addressed in greater detail in *Section VI*. It is imperative that data providers are afforded a reasonable amount of time to conduct due diligence on the third party, including its data security practices.

Additionally, the CFPB might allow data providers to enroll customers in a "no data sharing list" to create a rebuttable presumption that anyone seeking to access their data via a third party is a potential fraudster.

[28] *See* NPRM, supra note 2 at 1033.331(b)(1)(i) and 1033.331(b)(2).
[29] Id. at 1033.351(b)(2)(ii).

Moreover, the CFPB should encourage the creation of a non-binding (i.e., third parties are not required to seek accreditation nor are data providers obligated to rely on it) accreditation body that would register nonbanks that meet minimum standards for insurance, data security, compliance, etc. These would then be validated on an ongoing basis.

While accreditation by such a body would not qualify as a substitute for the third party risk management function,[30] it might serve as a non-exclusive indicia that the third party meets certain baseline criteria that would allow for an expedited due diligence process, subject to a bank's reasonable discretion. Banks operating as data providers would always reserve the right to place accredited entities that engage in questionable behavior under enhanced scrutiny. Unaccredited entities could still apply for access but must go through the full assessment. Such a construct would allow for banks to comply with prudentially required third party risk management functions to protect consumers and the financial system while simultaneously easing the onboarding process for vetted third parties to the extent possible.

Finally, the CFPB and the prudential regulators should be more transparent about any consultations that took place as required by the Section 1033 statute.[31] ABA also observes that the prudential regulators would be able to clarify expectations for their supervised entities through the release of guidance directly on this topic, with appropriate opportunity for stakeholder feedback.

III. The CFPB must not mandate that Section 1033 be used as a vehicle to initiate payments to and from a Regulation E account.

The CFPB must strictly construe Congress' grant of authority under Section 1033 and ensure that the personal financial data rights final rule is limited to facilitating access to consumer information, rather than extending it to effectuate transactions. In addition to the legal basis for this strict construction as laid out in *Section I*, there are strong policy reasons. The only way to make this use case viable would be to solve for liability. While ABA has long argued that liability should flow with the data[32] and the Director endorsed this view,[33] the NPRM insufficiently addresses liability (particularly with respect to payments initiation). More importantly, Section 1033 is not the appropriate vehicle to untangle and amend the many implicated laws and regulations. Therefore, the CFPB must strike those portions of the regulation that mandate enabling payments, such as the "information to initiate payment to or from a Regulation E account" data field.[34]

---

[30] It is important to note that banks do not choose to deal with a given third party under Section 1033—the interaction is purely a result of their customers' decision.
[31] U.S.C. 5533(e).
[32] *See* American Bankers Association, Response to ANPR of Proposed Rulemaking Regarding Consumer Access to Financial Records, https://www.aba.com/advocacy/policy-analysis/cfpb-anpr-consumer-access-to-financial-records.
[33] Testimony of Rohit Chopra, House Financial Services on CFPB Semi-Annual Report to Congress, November 29, 2023 ("We're trying to figure out under which of our statutes can we make sure absolutely clear that it's the receiving institution that really bears, you know, is responsible for handling that data").
[34] *See* NPRM, supra note 2 at 1033.211(c).

Keeping the mandate would allow payment initiation by unregulated or underregulated nonbanks that do not address consumer inquiries or disputes, provide notice of breach events, or practice sound third party risk management. Moreover, it would expand "pay-by-bank" to unfit and untested use cases, which could result in substantial consumer harm while posing risk to financial stability.

IV. The CFPB must permit recoupment of costs as a matter of public policy.

The fee prohibition applies to all data providers and ignores the very real costs associated with building and maintaining the consumer and developer interfaces required by the NPRM, which are severely underestimated in the CFPB's analysis. In essence, data providers are compelled under penalty of noncompliance to subsidize the business models of data aggregators and third parties seeking to monetize the information. It represents nothing less than a forced transfer of value. Therefore, there are strong policy reasons for removing the prohibition on fees in addition to the legal argument appearing in *Section I*.

The proposed prohibition on fees is especially unwarranted given that "consumer" is defined to mean "an individual or an agent, trustee, or representative acting on behalf of an individual"[35] and that data is to be made available in electronic (and machine readable) form.[36] Thus, this is not an ordinary sort of information sharing requirement, but introduces thorny questions of authorization, authentication, technological architecture, interoperability, and more; all of which imply cost to be incurred by the data provider.

Moreover, the only effective way to validate that data providers are adhering to a qualified industry standard (QIS) is for the issuer to offer a certification. Otherwise, entities would be able to make a unilateral claim they are following the standard but there will be limited ability to confirm (because the CFPB examiners will likely be unable to make this technical determination themselves). Such a certification would possibly entail fees and would represent another cost center for data providers. To prohibit reasonable cost recoupments, especially with regard to the developer interface, would ultimately be anti-competitive. An added benefit of assessing nominal fees is that it discourages fraud from bad actors who might otherwise engage in bulk collection or brute force tactics.

It is important to note that not all data providers will choose to recoup their costs. However, it is essential that they retain the ability to assess reasonable fees since this will allow them to make business decisions in accordance with their strategy and resources. In addition, it levels the playing field given that data aggregators and third parties are able to charge fees; it also applies to the entire ecosystem since an entity can be either a third party or a data provider depending on the situation.

Furthermore, we ask CFPB consideration of two dynamics likely to shape the market response to the 1033 rulemaking, which the prohibition on fees will exacerbate. First, the significant technology investments at large companies vastly outpaces that of smaller entities. Performing

[35] 12 U.S.C. 5481(4).
[36] 12 U.S.C. 5533.

data analytics requires more than merely having access to data; it also requires additional infrastructure and personnel, either obtained directly or by outsourcing. Second, this rule may put additional cost pressures on smaller depositories' management of consumer checking accounts, which is already challenged to achieve economies of scale.

ABA continues to be concerned about potential competitive impacts on financial institutions, including small banks. We urge the CFPB to consider the collective impact of the many rules put forth by federal regulators over the last several years and permit the recoupment of costs. This would help data providers, including small banks, thrive in the new regulated environment.

V. In the final rule, the CFPB must expressly state that data providers making information available pursuant to Section 1033 are deemed not to be furnishers under the Fair Credit Reporting Act.

In September 2023, the CFPB commenced the SBREFA process for FCRA rulemaking.[37] While not responding to that proposal here, ABA does wish to caution the CFPB that it is very dangerous to conduct simultaneous rulemaking activity on foundational matters that could yield momentous unintended consequences. The FCRA outline makes several references to data aggregators.[38] However, regardless of what happens with changes to FCRA, ABA members have expressed profound concern that the NPRM makes a reference to some data aggregators being regulated as consumer reporting agencies under the FCRA.[39]

This reference, which only appears in the preamble and not in the regulatory text, is alarming because the implication is that data providers in the Section 1033 ecosystem are thereby functioning as furnishers under the FCRA notwithstanding the fact that they have no choice but to hand over the information (outside a few inapplicable exceptions). FCRA carries massive compliance burdens for entities that choose to furnish. Consequently, some small banks elect not to furnish at all for this reason. These institutions would have to build out an entirely new workstream and compliance program. Other banks that are currently furnishers would see their compliance costs increase exponentially if this new realm of activity becomes subject to the FCRA.

In the final rule, the CFPB must expressly state that data providers making information available pursuant to Section 1033 are deemed not to be furnishers under the FCRA.[40]

---

[37] *See* Consumer Financial Protection Bureau, Small Business Advisory Panel for Consumer Reporting Rulemaking: Outline of Proposals and Alternatives Under Consideration (Sept. 15, 2023), https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-rule-sbrefa_outline-of-proposals.pdf.
[38] Id.
[39] *See* NPRM, *supra* note 2 at preamble.
[40] Furthermore, the Section 1033 final rule should not conflict with future Bureau activity, including rulemaking or guidance. To the extent there is existing overlap (such as with the CFPB's recent guidance on Section 1034(c)), the Bureau should provide additional information and context on the respective obligations. Moreover, the Section 1033 final rule should not impact forms of data sharing pursuant to other legal frameworks, such as GLBA.

VI. The CFPB should revise several sections of the regulatory text to avoid confusion or otherwise ensure the practical operationalization of the rule.

While many principles in the NPRM may appear reasonable in the abstract, they would prove unduly burdensome to implement or are simply too ambiguous to operationalize. This section is devoted to pointing out these challenges to the Bureau so that the related cost/benefit analyses are properly addressed in the final rule.

A. Standard-Setting

A key element of the June 2023 blog post was the CFPB's recognition that market-driven technical solutions were preferable to those imposed by the government. ABA was pleased to see this concept included in the NPRM as a "fair, open, and inclusive standard-setting body" and an "issuer of qualified industry standards."[41] Unfortunately, there is a great deal of ambiguity in the way these ideas were executed and there should be substantial improvement before the rule is finalized.

Although standards have evolved in the marketplace through the important work of the Financial Data Exchange (FDX), FDX was not directly addressed in the NPRM.[42] At this time, FDX seems to be the only viable entity that could be "deemed to satisfy" the concept of a broadly adopted standardized format for data exchange through the developer interface.[43] However, in light of the acknowledged lack of currently existing QIS, the fallback offered is unreasonably vague. This language directs a data provider to look to those who are "similarly situated,"[44] but it is unclear how a data provider (regardless of size) determines what is similarly situated or how to determine the design and functionality of their developer interfaces. If the reference to "similarly situated" is meant to suggest that the FDX standard may be followed in absence of a QIS, the final rule should clearly express this (perhaps incorporated by reference) lest the CFPB create ambiguity in the ecosystem. The market participants will only be able to build a developer interface and make covered data available if there is clarity in how to do so.

Other sections of the NPRM cite to a concept referred to as an "indicia of compliance."[45] It is not readily understood what this means. The Bureau should revisit and use a more familiar term such as a safe harbor. Importantly, the CFPB should also clarify that not following a QIS does not result in a presumptive violation due to the need to engage activities such as risk management and preserving prudential safety and soundness.

The CFPB should also clearly incorporate the concept of certification for issuers of QIS. This would be likely be necessary for Bureau examiners to use as a tool to determine if entities are eligible for deference when using the QIS. It will also facilitate accreditation bodies and streamline third party risk management processes.

---

[41] *See* NPRM, *supra* note 2 at 1033.141.
[42] *See* Financial Data Exchange, https://financialdataexchange.org/FDX/About/About-FDX.aspx.
[43] See NPRM, supra note 2 at 1033.311(b).
[44] Id.
[45] Id. at 1033.311, 1033.351, 1033.421.

Some concepts (such as policies and procedures, and developer interface performance) are not appropriate for a QIS.[46] Accordingly, these activities should not be delegated to a QIS; instead, the Bureau should require ecosystem participants to "act reasonably"—coupled with rigorous oversight by agencies, this would be both simple and effective.

The CFPB must also discuss what happens if a QIS loses its status—how will the participants approach this situation? Surely it would only occur after significant discussion and opportunity to remedy, but it is paramount that the ecosystem not be thrown into tumult due to good faith disagreements.

Finally, ABA calls for more clarity about the process and criteria the CFPB will use to evaluate applications for entities seeking to become issuers of QIS. The Bureau should commit to transparency in explaining its rationale and consider stakeholder feedback in making its determination.

B. Covered Data

As a general matter, the CFPB should include language to the effect that data providers are only required to make available covered data that they own or generate independently. This clarification would significantly reduce the challenges in obtaining certain tangential data from other entities while not unduly impacting the information at the heart of Section 1033.

In addition, the NPRM contains several fields of proposed covered data that are problematic. We have already addressed some of these, such as pending transaction information, information to initiate payment to or from a Regulation E account, and upcoming bill information. However, there are other fields the Bureau should revisit and amend for other reasons, primarily due to them causing confusion or being impractical to operationalize:

i. Authorized but not yet settled debit card transactions[47]- in addition to the ultra vires basis, the inclusion of pending data is likely to lead to consumer confusion since third parties do not always put the figures into the correct context (e.g., gas station or hotel authorizations that do not post as authorized).

ii. Transaction information[48]- the period of at least 24 months for historical transaction information is too lengthy. A more appropriate figure would be no more than 12 months, which would be consistent with most systems' storage of easily accessible information—otherwise, the data could not be obtained electronically in the ordinary course of business. In addition, transaction information about rewards credits that are accumulated as a result of using the product or service should be struck because rewards programs are either proprietary or partnerships among multiple companies.

[46] Id.
[47] Id. at 1033.201(b).
[48] Id. at 1033.211(a).

iii. Information to initiate payment to or from a Regulation E account" data field[49]- the policy reasons for excluding this category are discussed in *Section III*.

iv. Terms and conditions[50]- this category is not conducive to data sharing and is not an existing field in the current ecosystem. This information would be difficult to deliver via API calls since it is contained in legal documents rather than data fields. Most of this information is already subject to other regulations and is produced to consumers at account opening or on demand in other contexts, and it is not necessary to require it to be produced electronically under Section 1033. A further complication is that rewards programs are either proprietary or partnerships among multiple companies. For all these reasons, the Bureau should strike this entire category from the final rule.

v. Upcoming bill information[51]- in addition to being clearly ultra vires (due to it being future state and not retrospective as per the statutory text), this field is arduous to collect due to it residing at various vendors.

vi. Basic account verification information[52]- this is an unnecessary vector for fraud and would add little value to the ecosystem if delivered through a developer interface. The third party can obtain this information from the consumer directly (if it is in fact a legitimate consumer and not a fraudster). Sharing this data field is not worth the risk it introduces, especially if the Bureau removes the "[i]nformation to initiate payment to or from a Regulation E account" from covered data as it should.[53]

C. Exceptions

The CFPB opted for a narrow construction of the statutory exceptions in the NPRM, and in some cases the determinations should be revisited:[54]

i. The "rewards" data mentioned in the "transaction information" and "terms and conditions" covered data fields should fit under the "confidential commercial information" exception. These programs add significant value to data providers and would severely undercut competition if made available. The exception explains that "[i]nformation does not qualify for this exception merely because it is an input to, or an output of, an algorithm, risk score, or predictor."[55] However, if a party were to possess both inputs and outputs, it would be far easier to reverse engineer the process. Accordingly, the CFPB should expressly prohibit reverse engineering in the final rule.

[49] Id. at 1033.211(c).
[50] Id. at 1033.211(d).
[51] Id. at 1033.211(e).
[52] Id. at 1033.211(f).
[53] *See* id. at 1033.211.
[54] Id. at 1033.221.
[55] Id.

ii. Enriched data provided by services providers (which is not normally available directly to consumers) should not be subject to disclosure and should likewise fall under "confidential commercial information." Indeed, due to it being enabled by vendors it could also fit under the "required to be kept confidential by other law"—namely, contract law.

iii. The "fraud prevention" exception is unnecessarily narrow. Very little information is collected solely for fraud prevention and likely has multiple purposes but would have little value for being supplied to a third party (who themselves could collect it directly). For example, many of the fields in "Basic account verification information" are also utilized to mitigate fraud.[56] The Bureau should remove the "solely" qualifier and tie this exception category to a data provider's risk management obligations.

D. Operational Targets

Several metrics or operational targets applied to data providers are overly prescriptive or overly reliant on QIS and should be replaced with a requirement for the data provider to "act reasonably."

For example, ABA members have offered a great deal of feedback on the performance specifications and access cap parameters for the developer interface.[57] The NPRM is highly prescriptive in requiring a response rate of 99.5%, fulfilling or denying within 3,500 milliseconds, limiting of frequency restrictions, etc.,[58] which are not consistent with a data provider's parallel requirements to conduct risk management. A QIS can aid with an understanding of the average timeframes for certain entities, but these should only be consulted after the third party is onboarded and sufficiently vetted.

In addition to the risk management obligations, the 99.5% response rate is simply too high, especially in light of the Bureau's insistence on a no-fee framework. The current state allows for batch processing of API calls, but ABA is concerned that the construct of the NPRM might be used to require "real time" responses that would have a deleterious effect on data providers' ability to meet 99.5% overall. For a case study of an external event driving spikes in traffic, the CFPB should consult consumers attempting to track the status of their COVID stimulus payments. Reasonable access caps should be allowed for the developer interface (note: the NPRM referring to this subsection as an "Access cap prohibition" is misleading since it only prohibits unreasonable access caps).[59] The 99.5% response rate is rendered even more challenging by the calculation of fulfillments and denials and the ambiguity of whether denials for risk management reasons fall into the equation.

The NPRM mandates data providers to make certain disclosures, such as its performance specifications. They are currently written to require information to be made available by the 10th

[56] Id. at 1033.211(f).
[57] *See* id. at 1033.311(c).
[58] Id.
[59] Id.

calendar day of each month.[60] This seems excessive and should be revised to include a grace period, perhaps of 45 days, to allow sufficient time for appropriate adjustments to be made. The CFPB should also be more precise in its language in this section, as it is not immediately clear what information is intended to be visible to the public and what is reserved for third parties seeking access to the developer interface.

E. Consumer Interface

The CFPB must provide additional detail around its concept of the consumer interface.[61] This concept is at the core of the statute and yet is given too light of a treatment in the NPRM. Because several of the data fields are new, there is currently no example of a consumer interface in existence. The idea that consumers can press a "magic button" and obtain all this information should be weighed against the potential impact to data providers. The Bureau should also consider reasonable access caps lest direct consumer requests during an external event (recall the stimulus payment example) lead to denials of access to other customers or impose unmanageable technological burdens on data providers' infrastructures.

We would also note that not having a consumer interface is an exceedingly confusing litmus test for an exemption.[62] ABA supports a limited exception because market forces are such that consumers want to share their information via Section 1033 and being left outside that environment will only harm those institutions and their customers. However, it is unclear whether any business currently has a consumer interface as contemplated by the NPRM. As such, it creates a technical loophole that could harm the functioning of the final rule. A better approach would be to use traditional online banking (the ability to access an account via the internet or mobile app to check balances and conduct transactions) as the relevant offering that determines whether an entity is eligible to assert the exemption. This would exempt the truly niche business model the CFPB contemplates while leading to more predictable outcomes in the ecosystem.

F. Privacy

The need to protect consumer privacy is one of the chief factors necessitating the CFPB's rulemaking activity. Screen scraping's wholesale capture of data fields is among its most egregious attributes, and placing controls on the use of personal information is often a contentious issue in the negotiation of DAAs. The challenge here, as in so many areas, is the unlevel playing field between highly-regulated banks and unregulated or underregulated nonbanks. Banks are subject to robust supervision and are held accountable for maintaining a mature data governance program. This is not the case for most nonbanks.

[60] Id. at 1033.341.
[61] Id. at 1033.331(a).
[62] Id. at 1033.111(d).

Given this general lack of supervisory oversight, the Bureau elected to apply the "reasonably necessary" privacy provisions in the NPRM that are more stringent than the GLBA/Regulation P's "consent" exception.[63] The NPRM indicates that "[t]he third party will limit its collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service."[64] The third party is to provide a "brief description of the product or service that the consumer has requested"[65] but "the scope of the product or service is not defined by disclosures, which could be used to create technical loopholes by expanding the scope of the product or service the consumer requested."[66] Certain activities such as targeted advertising, cross-selling, and sale of covered data are mentioned as examples of activities not reasonably necessary to provide the requested product or service.[67] ABA understands that, historically, many nonbanks have utilized voluminous disclosures with inconspicuous terms or dark patterns to induce the granting of consent, and strongly supports restricting these activities.

While ABA supports the spirit of the provision, it is confusing how it will function in practice. Therefore, the Bureau should clarify its privacy expectations by providing examples of "brief description[s] of the product or service" (including developing its concept of a "stand-alone product" as referenced in footnote 130 of the preamble).[68] Similarly, the CFPB should provide additional context around data use prohibitions as many third parties are not held to bank-like standards for the use and sharing of consumer personal information. For example, the Bureau might specifically prohibit reverse engineering as a secondary use of data.

These additions will ease compliance by assisting with the creation and maintenance of effective data governance programs while still allowing for responsible innovation in a way that ultimately benefits consumers. An example of a use case that is to the consumer's advantage is a bank informing its customer that moving funds from a checking account to its high-yield savings account would result in greater interest payments.

Data aggregators should face even more stringent controls as a separate class because consumers have no meaningful choice—it is purely a business decision by the third party. Data aggregators are simply the intermediary to move data from the data provider to the authorized third party; as such, any treatment of the data by data aggregators other than transmitting or for the uses laid out in 1033.421(c) should be prohibited.

To be clear, the CFPB continues to bear the responsibility for monitoring and enforcing these privacy provisions for data aggregators and third parties (whether bank or nonbank). Data

[63] Id. at 1033.421(a); *See also* 12 C.F.R. 1016.15(a)(1): The requirements for initial notice in § 1016.4(a)(2), for the opt out in §§ 1016.7 and 1016.10, and for service providers and joint marketing in § 1016.13 do not apply when you disclose nonpublic personal information: (1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction.
[64] *See* NPRM, supra note 2 at 1033.421(a).
[65] Id. at 1033.411(b)(3).
[66] Id. at preamble.
[67] Id. at 1033.421(b).
[68] Id. at preamble.

providers are unequipped to do so, not only from an authority perspective but also because they do not have insight into how the data is used once it leaves their environment (although the ability to confirm the authorization scope or to offer a revocation mechanism does enable data providers to use optional privacy-enhancing levers).[69]

Finally, the CFPB must expound upon the status of data already in the ecosystem. Unless this is tackled, third parties will simply continue to use information already in their possession to do with as they like. It is imperative that the final rule lays out the CFPB's plan to protect consumers and participants who have been involved in these activities for many years prior to regulation.

G. Condition Precedent

ABA observes that, ideally, a QIS for the standardized formats should be established as the triggering mechanism for when the countdown to compliance begins. It should not simply be publication of the final rule in the Federal Register since that does not factor in resource allocations, budgeting process, the timeframes to create workstreams and documentation, or the nebulousness of building to a standard that may not deemed to be in compliance.[70] Thus, regardless of whether or not FDX is ultimately labeled a QIS, there must be clarity that the FDX standard will satisfy the developer interface in the immediate wake of the final rule. A lack of such clarity would lead to delays, conflicting or inadequate development standards, and would lack the needed level of interoperability as not all parties share the same risk appetite or resources.

H. Compliance Dates

Rather than apply to only data providers, the final rule should clearly require all participants to perform certain actions by clear timeframes. In any event, once a third party ingests a consumer's financial information it will become a data provider in its own right. Further, additional information is also needed for the sorts of penalties and actions that will result for noncompliance.

Regarding the subject of compliance timeframes, we appreciate the concept of tiers but recommend the CFPB revisit the deadlines, especially if they do end up including more account types. ABA has members that fall into each of the NPRM's compliance tiers, and all have expressed appreciation that their different circumstances were recognized. Nonetheless, questions and concerns remain.

The CFPB should also clarify how details such as ownership structure influence which tier an entity falls into as some entities are comprised of multiple types of companies (for example, a Regulation Z credit card issuer that falls into one tier and a Regulation E financial institution that falls in another). More guidance on this complicated corporate question is necessary.

[69] *See* id. at 1033.331(b) and 1033.331(e).
[70] Id. at 1033.121.

The largest banks with assets of at least $500 billion have a mere 6 months in which to comply per the NPRM.[71] This is far too short even if FDX is deemed to satisfy the standardized format of the developer interface because the NPRM introduces several completely new concepts. The difficulty would increase if new categories of information such as EBT data were included. ABA recommends that several of these new concepts be struck, but in any event the CFPB should revise the compliance date for the first tranche of data providers to 2 years after the later of: 1) standards to be deemed to comply are named; or 2) the final rule is published in the Federal Register. The other compliance tiers should be pushed back on a proportional timeframe.

In addition, the Bureau ignores the degree to which entities less than $50 billion will rely on third-party solutions, some of which may function as both data aggregators and service providers offering developer interfaces or data dashboards. These entities will be limited to the functionality offered by these third parties and would be beholden to the development timeframes provided to them. This is one of the reasons why the compliance dates should be applicable to all entities, not just data providers.

Depending on what recommendations the CFPB incorporates into its final rule, it should revisit the tiers in order to ease the burden while optimizing the chances for success.

I. Other Recommendations

ABA has several other recommendations for the CFPB to consider:

- Data providers already have existing procedures and channels for providing information to "natural" third parties (such as agents, attorneys, accountants, guardians, etc.), whether in electronic form or otherwise. These types of individuals should not be required to go through a developer interface. Accordingly, the CFPB should expressly exempt "natural" third parties from the scope of Section 1033.

- The final rule should include references that the electronic signature is intended to comport with ESIGN.[72] Moreover, the option for a wet signature should be removed as it is inconsistent with access to data in electronic form.

- ABA members have observed that the secondary language section in the authorization disclosure seems like a new direction for the CFPB and requires additional clarity on the ways UDAAP will apply to the provision of financial products and services on an end-to-end basis.[73]

- ABA believes that the third parties should have a more explicit requirement to delete data once authorization lapses or is revoked; the NPRM phrases this far too passively.[74] There should also be a provision in place allowing the consumer to close an account with the

[71] Id.
[72] Id. at 1033.401.
[73] Id. at 1033.411(c)(2).
[74] Id. at 1033.421.

third party upon request, which would include deletion of data not required to comply with law.

- Other areas in the NPRM in need of improvement include more practical retention obligations. Retention is a very complicated subject. The provisions in the NPRM are very formalized and onerous. Simply retaining workstreams and OAUTH logs should be sufficient, coupled with policies and procedures being in place. The time period of 3 years also seems excessive in light of the voluminous data that will be generated, and this would unduly strain the storage capacity of many systems for little demonstrable benefit.[75] The CFPB should be very clear in what information it expects to be retained under these requirements, and it should also reduce the duration to no more than 24 months.

- The CFPB should revisit the definitions section to make them less circular. In addition, ABA recommends that the CFPB add a definition of "machine-readable," and clarify that the right to request the format under 1033.301(b) applies to only a limited set of covered data fields to which it is suited (such as transaction information). Otherwise, this request as worded would introduce a new and costly set of requirements for data providers.

- The CFPB should clarify that the right to make requests under Section 1033 applies only to active accounts, as inactive/closed accounts have their own processes. The Bureau can implement this change by amending the definition of "consumer" by inserting "with at least one current/active account with the data provider,"[76] or alternatively by revising "covered consumer financial product or service,"[77] with CFPB guidance on what constitutes a current or active account to avoid inconsistent application.

- The Bureau should clarify that only accountholder(s) or their duly appointed representatives, and not authorized users, should be permitted to authorize requests pursuant to the regulation.

- The CFPB should provide model forms, compliance guidance, and other materials to assist small entities with understanding Section 1033 concepts and the obligations of respective participants under the final rule.

Conclusion

ABA and our members appreciate the CFPB's efforts to date in creating a new data sharing ecosystem, leveraging the foundation laid by the market. We believe that some of the concepts the CFPB has articulated could prove enduring but much more remains to be done to achieve fair, appropriate, and responsible regulation.

[75] Id. at 1033.351(d) and 1033.441.
[76] Id. at 1033.131.
[77] Id. at 1033.111(b).

Such an end can only happen if the Bureau acts prudently, taking its time to weigh and incorporate feedback from stakeholders. The work is too important to rush. The CFPB should not settle for merely "good enough." Consumers and ecosystem participants deserve better.

If you have any questions about this comment, please contact Ryan T. Miller (rmiller@aba.com) at (202) 663-7675.

Respectfully submitted,

Ryan T. Miller
Vice President & Senior Counsel, Innovation Policy