



**Innovative Payments Association**

110 Chestnut Ridge Rd, Suite 111

Montvale, NJ 07645

[btate@ipa.org](mailto:btate@ipa.org)

December 20, 2023

**Submitted via E-Mail at:** [2013-NPRM-Data-Rights@cfpb.gov](mailto:2013-NPRM-Data-Rights@cfpb.gov)

Financial Data Rights, C/O  
Legal Division Docket Manager  
Consumer Financial Protection Bureau  
1700 G Street, NW  
Washington, DC 20552

Re: Proposed Rule on Financial Data Rights  
[Docket No. CFPB-2023-0052]

To whom it may concern:

This letter is submitted to the Consumer Financial Protection Bureau (the "**CFPB**") on behalf of the Innovative Payments Association ("**IPA**"),<sup>1</sup> in response to the Proposed Rule on Personal Financial Data Rights issued by the CFPB on October 19, 2023 and published in the Federal Register on October 31, 2023 (the "**Proposed Rule**").<sup>2</sup> The IPA's members appreciate the opportunity to comment on this important rulemaking that will have impacts on covered financial institutions, third party data processors, and consumers. We note that the Proposed Rule includes a number of highly technical elements and requirements. We have provided some comments to specific requests for comment from the CFPB below, but, at the outset, wish to first outline a few overarching concerns on the Proposed Rule that we ask the CFPB to consider while developing a final rule.

*The CFPB should provide a safe harbor from liability for data providers that make covered data available in compliance with the rules*

The Proposed Rule requires covered data providers – those offering accounts subject to the Electronic Fund Transfer Act and Regulation E, credit cards under the Truth in Lending Act, and related payment facilitation products and services – to make covered data related to such products and services available to both the consumer that has acquired the covered product and to the consumer's authorized third parties. "Covered data" includes highly sensitive, non-public customer information including (i) transaction information, (ii) account balances, (iii) terms and conditions for the account, (iv) information on upcoming bill payments, and (v) account verification information such as name, address, email, and phone number.

---

<sup>1</sup> The IPA is a trade organization that serves as the leading voice of the electronic payments sector, including prepaid products, mobile wallets, and person-to-person (P2P) technology for consumers, businesses and governments at all levels. The IPA's goal is to encourage efficient use of electronic payments, cultivate financial inclusion through educating and empowering consumers, represent the industry before legislative and regulatory bodies, and provide thought leadership. The comments made in this letter do not necessarily represent the position of all members of the IPA.

<sup>2</sup> 88 Fed. Reg. 74796 (Oct. 31, 2023).



Given the sensitive and personal nature of "covered information," the potential that such information could either be abused or exploited by fraudsters or otherwise result in liability or increased scrutiny of the data provider is very high. Our members are thus concerned that the requirement to make such "covered data" available on demand to a consumer and the consumer's authorized third party potentially exposes providers to significant additional risks simply by complying with their obligations under the rule.

One example of increased risks comes from a third party either fraudulently obtaining authorization to access such information, or an authorized third party exceeding the scope of what information they could access and/or how that information could be used. While the Proposed Rule contains provisions to mitigate these risks, such as the ability of the data provider to confirm a third party's authorization with the consumer, we note that such mitigating factors do not eliminate the risk entirely. For example, a confirmation of authorization would not protect the data provider from claims that the consumer was tricked into granting that authorization by a fraudster and the consumer's seeking to hold the data provider responsible for any resulting damages.

Further, sharing covered information even without the potential risk for fraud, may potentially expose data providers to risks of liability and scrutiny. For example, consider a case where a data provider holding an account covered by Regulation E shares covered data, and the customer has one or more holds on their account at the time of the request. As a result of the hold or holds on the account, the information provided may not accurately reflect the customer's current financial state and lead to negative outcomes such as an overdraft or NSF fee, which in turn exposes the data provider to increased potential liability and regulatory scrutiny.

Based on these risks, we believe additional action is necessary to ensure that providers that make "covered data" available to a consumer and their authorized third party are not faced with an increase in liability simply from complying with the rule. For this reason, we request that the CFPB provide a safe harbor from liability as part of a final rule for data providers that make covered data available to a consumer and their authorized third parties in compliance with the requirements of the rule.

*Concern over potential increases in fraud stemming from the Proposed Rule*

Closely related to the increases in liability for data providers complying with covered data requests under the Proposed Rule, is the more generalized risk of increased fraud or abuse given the sheer amount of data that will move between data providers and authorized third parties under the rule's requirements. Our members urge the CFPB to work with other prudential regulators as well as industry standards organizations such as the National Institute of Standards and Technology (NIST) on affirmative steps that may be taken – without further increasing the complexity of the rule – in order to minimize the risks of fraudsters and other persons or entities from abusing or otherwise exploiting the final rule.

*Concern over the interplay and potential for conflict of the Proposed Rule and state privacy laws*

An additional aspect of the Proposed Rule our members have expressed concern over is the interaction between certain requirements of the Proposed Rule and what may be conflicting obligations under state privacy laws. Specifically, we note that several of the Proposed Rule's obligations for authorized



**Innovative Payments Association**

110 Chestnut Ridge Rd, Suite 111

Montvale, NJ 07645

[btate@ipa.org](mailto:btate@ipa.org)

third parties mirror many common requirements of state privacy laws such as the California Consumer Privacy Act ("CCPA"). Common requirements mirrored by the obligations in the Proposed Rule include the consumer's express and informed consent, the requirement for the third party to limit the scope of use of consumer data to what is necessary to provide the third party's service and to delete such data once that purpose has expired.

Given the overlap between the obligations under the Proposed Rule and the common requirements of state law, our members are concerned with the potential for conflict where complying with the requirements of one set of obligations may cause a covered person or entity to violate the others. This concern is exacerbated by the fact that data privacy, and the development of state level consumer privacy protection frameworks in particular, is an evolving sector with an already challenging and complex array of differing, and sometimes contradictory, requirements for providers to navigate. Adding a federal framework for providers to grapple with only increases the risk of potential violations stemming from efforts of providers to comply.

For this reason, we urge the CFPB to take further consideration of state level privacy requirements into account as part of its rulemaking process and to consider the need for clarity in how providers navigate and comply in this increasingly complex area.

*Treatment of Data Aggregators*

With respect to the treatment of data aggregators, we note that the Proposed Rule generally defines data aggregators as entities retained by authorized third parties to enable access to covered data. The Proposed Rule imposes certain obligations on data aggregators directly, including a separate requirement for a data aggregator to certify to a consumer that the data aggregator agrees to the relevant conditions on accessing that consumer's covered data. Our members note that there is a wide range of operating models and services provided by data aggregators and implementation of rules concerning data aggregators may impact that may have an impact on data providers' own compliance with the requirements of the Proposed Rule. As such, we respectfully request that the obligations of data providers in the Proposed Rule should not be required until any data aggregator rules are also finalized and implemented.

**SPECIFIC REQUESTS FOR COMMENT FROM CFPB AND IPA RESPONSES**

Finally, we note that the Proposed Rule includes a number highly technical elements and requirements and, accordingly, the CFPB has included a number of requests for comments within the Proposed Rule to address these elements. We have provided responses to certain of those requests for comment below:

**Implementation Period**

Request from CFPB: The Proposed Rule contains tiers of compliance dates for data providers (e.g., six months, one year, two-and-one-half years, and four years from the publication of the final rule depending on size of depository institution and revenue of non-depository institution).



**Innovative Payments Association**

110 Chestnut Ridge Rd, Suite 111

Montvale, NJ 07645

[btate@ipa.org](mailto:btate@ipa.org)

- Regarding these tiers, should additional criteria such as a provider's number of accounts be considered?
- Comments generally to structure of each tier and whether non-depository data providers should be included?

IPA Response: Given the highly technical nature and requirements of the Proposed Rule, our members anticipate a significant amount of development and operations time will be needed in order to ensure compliance. While we recognize that the tiers proposed by the CFPB seek to take into account the available resources and technical capabilities of covered providers of different sizes, we believe the proposed timelines miss the mark. The sheer size and complexity of the existing operations of larger covered providers may in some circumstances require more time to design and implement changes required by the Proposed Rule, not less. For instance, much of this work cannot begin until the standard file formats contemplated by the Proposed Rule are finalized.

Given these considerations, rather than a tiered approach based on the size of the covered provider that could range anywhere from six months to four years, we recommend that the final rule implement a single implementation timeline of two years for all covered providers, and that this implementation period be cued from the date the standard file formats are finalized. This will create a level implementation playing field for all covered providers and ensure a sufficient amount of time to modify and implement processes for compliance.

### **Assessment of Cost for Providing Covered Data**

Request from CFPB: Whether any clear and unambiguous set of conditions, limitations, or other parameters exist or should be created such that data providers could charge reasonable, standardized fees that neither obstruct the access right due to cost nor impede third parties' access to data provider interfaces due to negotiations over fee amounts or schedules?

IPA Response: Our members believe it is reasonable to allow covered data providers to assess at a minimum, a de minimis fee to an authorized third party to help recoup the cost needed to establish, maintain, and support the data provider interfaces and other processes needed to comply with the rule's requirements.

We would thus support the CFPB's clarification as part of the final rule, that providers may assess such a fee to any authorized third party seeking access to the data providers' interfaces.

The IPA appreciates your consideration of these comments. If you have any questions or wish to discuss this letter, please do not hesitate to contact me at: [btate@ipa.org](mailto:btate@ipa.org).



**Innovative Payments Association**

110 Chestnut Ridge Rd, Suite 111

Montvale, NJ 07645

[btate@ipa.org](mailto:btate@ipa.org)

Sincerely,

A handwritten signature in black ink, appearing to read 'Brian Tate', is written over a solid horizontal line.

Brian Tate  
President and CEO

IPA

[btate@ipa.org](mailto:btate@ipa.org)