zeta Whitepaper

Personal Financial Data Rights

Delivering consent-driven customer data access under Section 1033

December 2023

Contents

Proposed Rules for Personal Financial Data Rights: Summary

The Consumer Financial Protection Bureau (CFPB) is proposing to establish 12 CFR part 1033, to implement section 1033 of the Consumer Financial Protection Act of 2010 (CFPA). The proposed rule would require depository and nondepository entities to make available to consumers and authorized third parties certain data relating to consumers' transactions and accounts; establish obligations for third parties accessing a consumer's data, including important privacy protections for that data; provide basic standards for data access; and promote fair, open, and inclusive industry standards.

The CFPB is expected to issue the final rule in November 2024 with effective dates for implementation beginning six months after. The CFPB is proposing to provide a longer compliance period for the smallest depository institution data providers.

The CFPB is proposing to first apply part 1033 to a subset of covered persons—namely, entities providing asset accounts subject to the Electronic Fund Transfer Act (EFTA) and Regulation E, credit cards subject to the Truth in Lending Act (TILA) and Regulation Z, and related payment facilitation products and services. This is intended to prioritize some of the most beneficial use cases for consumers and leverage data providers' existing capabilities.

The proposed regulations seek to ensure that consumers can access covered data in an electronic form from data providers. They would additionally address challenges concerning the open banking system by delineating the scope of data that third parties can access on a consumer's behalf, the terms on which data are made available, and the mechanics of data access.

The proposed regulations also would ensure that third parties act on consumers' behalf when collecting, using, or retaining data.

Key Objectives

If finalized as proposed, this rule will foster a data access framework that is:

- Safe, by ensuring third parties are acting on behalf of consumers when accessing their data, including concerning consumers' privacy interests;
- Secure, by applying a consistent set of security standards across the market;
- Reliable, by promoting the accurate and consistent transmission of data that are usable by consumers and authorized third parties; and
- Competitive, by promoting standardization and not entrenching the roles of incumbent data providers, intermediaries, and third parties whose commercial interests might not align with the interests of consumers and competition generally.
- The proposed definition of covered data would ensure consumers have access to key pricing terms, transaction and balance information, payment initiation information, and terms and conditions. This would facilitate consumer choice, including the ability of consumers to change providers of products or services.

Clarifying the scope of the data rights also would promote consistency in the data made available to consumers, reduce the costs of negotiating the inclusion of such data in access agreements, and focus the development of technical standards around such data.

The proposed framework is intended to foster a safe, secure, reliable and competitive framework by direct regulation of market practices, as well as identifying areas in which fair, open and inclusive standards can develop to provide additional guidance to the market.

Key Requirements from Data Providers

Establishing basic standards for data access

The proposed rule would require data providers to establish and maintain a developer interface for third parties to access consumer-authorized data. Developer interfaces would need to make available covered data in a standardized format, in a commercially reasonable manner, without unreasonable access caps, and under certain security specifications.

In addition, data providers would need to follow certain procedures to disclose information about themselves and their developer interfaces, which would ensure that consumers and authorized third parties have the information necessary to make requests and use the developer interface. Data providers also would be required to establish and maintain written policies and procedures to promote these objectives. Altogether, these provisions would ensure data providers make data available reliably, securely, and in a way that promotes competition.

Transitioning the market from screen scraping

The proposed rule would prevent data providers from relying on screen scraping to comply with the proposal because it is not a viable long-term method of access. Instead, data providers would be required to establish and maintain developer interfaces that would make data available in a machine-readable, standardized format and could not allow a third party to access the system using consumer interface credentials.

> While the CFPB is not proposing amendments to Regulation E at this time, proposed part 1033 contains multiple provisions that would reduce fraud and unauthorized access risk in the open banking system.

Clarifying the mechanics of data access

The CFPB is proposing certain requirements and clarifications to implement CFPA section 1033 concerning when a data provider must make available covered data upon request to consumers and authorized third parties. These provisions include:

- requiring that third-party access be effected through a developer interface (rather than through credential-based screen scraping);
- prohibiting a developer interface from requiring a third party to obtain or possess credentials for the consumer interface; and
- allowing data providers to share tokenized account and routing numbers.
- allowing data providers to restrict access to their developer interface when they have reasonable risk management grounds to do so

Ensuring third parties are acting on behalf of consumers

To effectuate consumers' control of access to their data, the proposed rule contains provisions intended to ensure that when consumers authorize a third party to access data on their behalf, the third party is actually doing so. To that end, the proposed rule would require a third party to certify to consumers that it will only collect, use, and retain the consumer's data to the extent reasonably necessary to provide the consumer's requested product or service.

The proposed rule also would aim to improve consumers' understanding of third parties' data practices by requiring a clear and conspicuous authorization disclosure including key facts about the third party and its practices. Other key protections in the proposed rule include limiting the length of data access authorizations and requiring the deletion of consumer data in many cases when a consumer's authorization expires or is revoked.

Separately, the proposed rule would exercise the CFPB's authority to define financial products or services under the CFPA to ensure that it includes providing financial data processing. Although the CFPB has tentatively concluded that this activity would qualify as a financial product or service without a CFPB rule, this rule provision would provide additional assurance that financial data processing by third parties or others is subject to the CFPA and its prohibition on unfair, deceptive, and abusive acts or practices.

Promoting fair, open, and inclusive industry standards

Industry standard-setting bodies that operate in a fair, open, and inclusive manner have a critical role to play in ensuring a safe, secure, reliable, and competitive data access framework. Accordingly, indicia of compliance with various provisions in the rule, if finalized as proposed, would include conformance with standards promulgated by the fair, open, and inclusive standard-setting bodies recognized by the CFPB.

To help support and maintain a data access framework that enables consumer access in a consistently safe, reliable, and secure manner across the market, industry standards must be widely adopted.

To meaningfully scale, standards must reflect a diverse set of interests, increasing the likelihood that market participants will adopt the standards and maintain their integrity. Conversely, if standards are controlled by dominant incumbents or intermediaries, they may enable rent extraction and cost increases for smaller participants.

Fair, open, and inclusive standard-setting bodies are vital to promote standards that can support a data access system that works for consumers, rather than the interests of dominant firms.

Implementation Considerations and Systems Impact

Key Objective	Implementation Considerations	Systems Impact
Establishing standards for data access	Establish and maintain developer interfaces for third parties to access consumer-authorized data. Make developer interfaces accessible and usable by third parties.	• **Headless architecture** • **Comprehensive API stack** • **Low code configurability** • **BaaS readiness with flow of data and actions across multiple systems**
Transitioning from screen scraping to well-defined mechanics of data access	Make authorized consumer data available in a standardized, machine-readable format from developer interfaces. Not require consumer interface credentials to access consumer data through developer interfaces, and share tokenized account and routing numbers with third parties. Revoke or restrict third-party access to developer interface upon sufficient risk management grounds	• **Flexible and extensible data models for enrichment and standardization across systems** • **Ability to define and control third-party API access**
Ensuring third parties are acting on behalf of consumers	Deliver a clear and conspicuous authorization disclosure including key facts about the third party and its practices. Limiting the length of data authorizations and requiring the deletion of consumer data when a consumer's authorization expires or is revoked.	• **BaaS readiness with integration of data and actions across multiple systems** • **Use of event streams and interceptors across integrations to control/ validate flow of data and actions in real-time**
Promoting fair, open and inclusive industry standards	Compliance with fair, open and inclusive industry standards that can support a data access system that works for consumers	• **Flexible and extensible data models** • **BaaS readiness with integration of data and actions across multiple systems**

Appendix

Analysis of Proposed Rule Making

Proposed institutional coverage

Entity	Description of proposed rule	Location in the proposed rule
Covered data providers	A covered data provider would be a covered person (as defined in 12 U.S.C. 5481) that: • Is a financial institution, as defined in Regulation E,1 and controls or possesses covered data (see below) concerning a covered consumer financial product or service (see below); • Is a card issuer, as defined in Regulation Z,2 and controls or possesses covered data concerning a covered consumer financial product or service; or • Controls or possesses information concerning a covered consumer financial product or service the consumer obtained from that person, and also controls or possesses covered data concerning any covered consumer financial product or service. Depository institutions that do not have a consumer interface as of the otherwise applicable compliance date would not be covered data providers under the proposed rule. A consumer interface w in ould be an interface through which a data provider receives requests for covered data and makes available covered data in an electronic form usable by consumers in response to their requests.	**1033.111(a), ©, and (d), 1033.131**

Other parties affected by the proposed rule

Entity	Description of proposed rule	Location in the proposed rule
Consumer	Consumer would mean a natural person, including a trust established for tax or estate planning purposes.	**1033.131**
Third-party	A third party would be a person or entity that is not the consumer whose data is being accessed or the data provider making the data available.	**1033.131**
Authorized third party	An authorized third party would be a third party that: • Seeks access to covered data from a data provider on behalf of a consumer to provide a product or service the consumer requested, and • Has complied with the other authorization procedures in the proposed rule (see below).	**1033.131** **See also 1033.401**
Data aggregator	A data aggregator would be an entity that is retained by and provides services to an authorized third party to enable access to covered data.	**1033.131**

Proposed covered products, services and data

Entity	Description of proposed rule	Location in the proposed rule
Covered consumer financial product or service	A covered consumer financial product or service would be a consumer financial product or service (as defined in 12 U.S.C. 5481(5)) that is also: An account, as defined in Regulation E (i.e., a Regulation E account); A credit card, as defined in Regulation Z (i.e., a Regulation Z credit card); or The facilitation of payments from a Regulation E account or Regulation Z credit card.	**1033.111(b)**
Covered data	Covered data would mean: • Transaction information, including historical transaction information in the control or possession of the data provider; • Account balance; • Information to initiate payment to or from a Regulation E account; • Terms and conditions (e.g., 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); • Upcoming bill information (e.g., information about third-party bill payments scheduled through the data provider and any upcoming payments due from the consumer to the data provider); and • Basic account verification information (limited to the name, address, email address, and phone number associated with the covered consumer financial product or service). Covered data would not include • Confidential commercial information; • Information collected by the data provider for the sole purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct; • Information required to be kept confidential by any other provision of law; or • Information that the data provider cannot retrieve in the ordinary course of its business.	**1033.211,** **1033.221**

Proposed requirements for covered data providers

Topic	Description of proposed rule	Location in the proposed rule
Making covered data available upon request in electronic form; interface access	A covered data provider would be required to make available to a consumer and an authorized third party, upon request, covered data in the data provider's control or possession concerning a covered consumer financial product or service that the consumer obtained from the data provider. The data provider would be required to make the covered data available in an electronic form usable by consumers and authorized third parties. Generally, the covered data provider would be required to provide this covered data through a consumer interface or developer interface, as discussed below. The covered data provider would provide consumers and third parties with access to the applicable interface and respond to their requests for covered data through that interface. However, a covered data provider would not violate this general obligation to make covered data available upon request if it reasonably denies a consumer or third party access to an interface based on risk management concerns as detailed in the proposed rule. If a covered data provider denies access to a third party, the data provider would be required to document the basis for the denial and communicate with the third party about the denial as quickly as practicable.	**1033.201, 1033.321, 1033.351(b)(2)**

Topic	Description of proposed rule	Location in the proposed rule
Establishing and maintaining interfaces	A covered data provider would be required to have a consumer interface and a developer interface (an interface that a data provider establishes and maintains to receive requests for covered data and make covered data available to authorized third parties). Both the consumer interface and developer interface would have to make available, upon request, covered data in a machine-readable file that can be retained by a consumer or authorized third party and transferred for processing into a separate information system that is reasonably available to and in the control of the consumer or authorized third party. The developer interface would have to satisfy additional standardized format, performance, and security requirements outlined in the proposed rule. Generally, a covered data provider would be required to make covered data available to a consumer when the data provider receives a request from the consumer and sufficient information to authenticate the consumer's identity, and identify the scope of the data that the consumer has requested. Similarly, a covered data provider would be required to make covered data available to a third party when it receives the third party's request and information sufficient to authenticate the consumer's and the third party's identities, confirm the third party has followed the authorization procedures in the proposed rule, and identify the scope of the data that the third party has requested.	**1033.131, 1033.301, 1033.311**
Responding to request	However, a covered data provider is not required to make covered data available when the data provider would have a basis to deny access to the interface for risk management concerns as detailed in the proposed rule, or the data provider's interface is not available when it receives the request (subject to the performance requirements in the proposed rule). Additionally, a covered data provider is not required to make covered data available in response to a third party's request when the third party is no longer authorized to access covered data. If a covered data provider denies a request from a consumer or third party, the data provider would be required to document the basis for the denial and communicate with the consumer or third party (as applicable) about the denial as quickly as practicable.	**1033.331, 1033.351(b)(3)**

Topic	Description of proposed rule	Location in the proposed rule
Fees prohibited	A covered data provider would be prohibited from imposing any fees or charges on a consumer or authorized third party in connection with: • Establishing or maintaining the interfaces required by the proposed rule; or • Receiving requests or making available covered data in response to requests as required by the proposed rule	**1033.301©**
Making certain information readily identifiable	The proposed rule would require a covered data provider to make certain identifying information readily identifiable to members of the public (e.g., disclose it to the public by putting the information on its website). The information would have to be available in both human-readable and machine-readable formats. A covered data provider would also be required to disclose to the public certain information about its developer interface and the quantitative minimum performance specification (as described in the proposed rule) that its developer interface achieved in the previous month	**1033.341**
Policies and procedures; record retention	A covered data provider would be required to have written policies and procedures reasonably designed to achieve the proposed rule's objectives including ensuring that covered data are made available in compliance with the proposed rule, ensuring that covered data are accurately made available, and ensuring retention of certain records.	**1033.351**

Proposed standard-setting provisions

Topic	Description of proposed rule	Location in the proposed rule
Qualified industry standard	A "qualified industry standard" would mean a standard issued by a standard-setting body that is fair, open, and inclusive in accordance with proposed -1033.141(a). Indicia of compliance with certain provisions of the proposed rule would include conformance with a qualified industry standard. There is one instance in which this would differ. If a covered data provider's developer interface makes covered data available in a format that is set forth in a qualified industry standard, the interface would be deemed to satisfy the proposed requirement that a developer interface use a standardized format.	**1033.131,** **1033.141**

Proposed provisions for authorized third-parties and data aggregators

Topic	Description of proposed rule	Location in the proposed rule
Authorization procedures	To satisfy the authorization procedures in the proposed rule, a third party would have to seek access to covered data on behalf of a consumer to provide a product or service the consumer has requested and: • Provide a written authorization disclosure that includes the key terms of access to the consumer on whose behalf it would access covered data; • Provide a statement in the authorization disclosure certifying that the third party agrees to certain obligations; and • Obtain the consumer's express informed consent to access covered data by having the consumer sign the authorization disclosure electronically or in writing (see below regarding the authorization disclosure, certification statement, and third party obligations).	**1033.401**
Authorization disclosure, and certification statement	The authorization disclosure (discussed above) would have to identify the data provider that controls or possesses the consumer's covered data, and the third party that will be authorized to access the covered data, the categories of covered data that the third party would be authorized to access. It would have to include a brief description of the product or service that the consumer requested from the third party, a statement that the third party will collect, use, and retain the consumer's data only for the purpose of providing that product or service to the consumer, and a description of a mechanism that the third party provides so that the consumer can revoke the third party's authorization to access covered data. The authorization disclosure also would have to include a certification statement, which is a statement by the third party seeking authorization certifying that it agrees to certain third-party obligations (see below regarding these third-party obligations).	**1033.411** **See also 1033.401,** **1033.421**

Entity	Description of proposed rule	Location in the proposed rule
Satisfaction of third-party obligations	• A third party would have to certify its agreement to certain third-party obligations in order to be an authorized third party. These third-party obligations would include: • Adhering to the proposed limitations on the collection, use, and retention of covered data; • Establishing, maintaining, periodically reviewing, and updating (as appropriate) policies and procedures to ensure that covered data is accurately transmitted; • Applying an information security program that satisfies section 501 of the Gramm Leach Bliley Act to its systems for the collection, use, and retention of covered data; • Providing consumers with copies of their authorization disclosures, information about the third party's access to their covered data, and third-party contact information. • Providing a mechanism that the consumer can use to revoke the third party's authorization to access covered data. The mechanism must be as easy to access and operate as the initial authorization. • • Additionally, a third party with authorization to access to covered data would have to certify that it will contractually require other third parties to comply with certain obligations (including limits on collection, use, and retention of covered data) before providing covered data to them.	**1033.421**
Use of data aggregators	When a third party will use a data aggregator to assist with accessing covered data, the third party would be permitted to use a data aggregator to perform the authorization procedures outlined in the proposed rule. The authorization disclosure would need to identify a data aggregator that assists a third party in accessing covered data and describe the data aggregator's services. The data aggregator would need to certify to the consumer that the data aggregator agrees to certain conditions for accessing the consumer's data (as detailed in the proposed rule).	**1033.431** **See also 1033.401, 1033.411**

Reference :
CFPB, Notice of Proposed Rulemaking - Required Rulemaking on Personal Financial Data Rights, November 2023

About Zeta

Zeta is a next-gen card processor. Zeta's platform empowers issuers to launch next-gen credit card programs with its cloud-native and fully API-enabled stack that includes processing, issuing, lending, core banking, fraud, loyalty, and many other capabilities. **Zeta** has 1700+ employees & contractors with over 70% in technology roles across locations in the US, UK, Middle East, and Asia. Globally, 35+ customers have issued 15M+ cards on Zeta's platform. Zeta has raised $280 million from Softbank Vision Fund 2, Mastercard, and other investors at a $1.5 billion valuation.

Connect with us

Karla Booe
Chief Compliance Officer, Zeta

Gary Singh
President, Banking
Zeta