Fast Facts: Personal Financial Data Rights Proposed Rule

Background on the proposed rule: The proposed rule would implement section 1033 of the Consumer Financial Protection Act of 2010 (CFPA or Dodd-Frank Act).

Proposed compliance date: The proposed rule would have tiered compliance dates. The earliest of the four compliance dates would be approximately 6 months after publication of a final rule in the *Federal Register*, and the last of the four compliance dates would be 4 years after publication of a final rule in the *Federal Register*. Generally, covered data providers that are larger depository institutions or that are nondepository entities would be required to comply earlier than covered data providers that are smaller depository institutions.

Comments due: Comments due by December 29, 2023.

Available at: www.consumerfinance.gov/rules-policy/rules-under-development/required-rulemaking-on-personal-financial-data-rights/.

About this document: This document generally provides a high-level overview of the topics covered in the proposed rule.

Proposed institutional coverage

Entity	Description in proposed rule	Location in 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	1033.111(a), (c), and (d), 1033.131

[1] 12 CFR 1005.2(i).

[2] 12 CFR 1026.2(a)(7).

Entity	Description in proposed rule	Location in proposed rule
	▪ 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 would 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.	

Other affected parties under the proposed rule

Other affected party	Description in proposed rule	Location in 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

	Description in proposed rule	Location in 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);[3] ▪ A credit card, as defined in Regulation Z (*i.e.*, a Regulation Z credit card)[4]; 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;	1033.211, 1033.221

[3] 12 CFR 1005.2(b).

[4] 12 CFR 1026.2(a)(15)(i).

	Description in proposed rule	Location in proposed rule
	▪ 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.	

Key requirements proposed for covered data providers

Topic	Proposed rule provisions	Location in 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	Proposed rule provisions	Location in 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 set forth in the proposed rule.	1033.131, 1033.301, 1033.311
Responding to requests	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. 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	1033.331, 1033.351(b)(3)

Topic	Proposed rule provisions	Location in proposed rule
	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.	
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(c)
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

Key proposed standard-setting provisions

Topic	Description of provision in proposed rule	Location in 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

Key provisions proposed for authorized third parties and data aggregators

Topic	Description in proposed rule	Location in 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	The authorization disclosure (discussed above) would have to identify the data provider that controls or possesses the	1033.411

Topic	Description in proposed rule	Location in proposed rule
certification statement	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).	See also 1033.401, 1033.421
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 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

Topic	Description in proposed rule	Location in proposed rule
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 set forth in the proposed rule. The authorization disclosure would need to identify a data aggregator that assists a third party 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 on accessing the consumer's data (as detailed in the proposed rule).	1033.431 See also 1033.401, 1033.411
Record retention	An authorized third party or a data aggregator that is a covered person or service provider (as defined in 12 U.S.C. 5481) would be required to have written policies and procedures that are reasonably designed to ensure retention of certain records.	1033.441

Additional resources

Additional resources related to the Personal Financial Data Rights Proposed Rule are available at www.consumerfinance.gov/rules-policy/rules-under-development/required-rulemaking-on-personal-financial-data-rights/.