KPMG

Regulatory Alert

Regulatory Insights for Financial Services

October 2023

"Open Banking" 1033 Personal Financial Data Rights – CFPB Proposal

Regulatory Insights:

- ***Controlling Your Data:*** *CFPB proposes to give consumers more control over their personal financial data as part of "Open Banking"*
- ***Bank/Nonbank Application:*** *Depository and non-depository entities would be subject to the rule*
- ***Current/Future Rules:*** *Deposit accounts and credit card accounts in current proposal; other products and services to be considered in future rulemakings*
- ***Focus on Security, Privacy, Protection:*** *Requirement for multi-layer authorization to promote consumer awareness, express consent, data protection*
- ***Data Minimization:*** *Requirements to limit data access, use, retention and authorization*

The Consumer Financial Protection Bureau (CFPB) proposes a rule to implement Section 1033 of the Consumer Financial Protection Act (2010), commonly referred to as "Open Banking". The rule would require depository and non-depository entities to share consumer financial data (relating to transactions and accounts) with both consumers and authorized third parties and would establish requirements for third parties accessing the data, including privacy protections and standards for access.

The proposal is outlined below.

A. Proposed Coverage

Coverage of Data Providers. The proposed rule would apply to entities that control or possess covered data concerning a covered financial product or service including financial institutions providing "Regulation E asset accounts" (e.g., checking, savings), card issuers providing "Regulation Z credit cards", and other providers of products or services that facilitate payments from a Regulation E account or a Regulation Z credit card (collectively, "data providers").

- *Note:* The proposed rule notes that digital wallet providers are generally considered Regulation E financial institutions and sometimes also as Regulation Z card issuers.
- *Note:* CFPB is considering whether to add electronic benefit transfer (EBT) card data to the final rule or a subsequent rulemaking and is seeking public comment on the topic.

Excluded Data Providers. The proposed rule would exclude data providers that do not have a consumer interface, or "an interface maintained to receive requests for covered data and make available covered data in an electronic form usable by consumers in response to the requests", as of the applicable compliance date.

B. Proposed Obligation to Make Covered Data Available

Covered Data Availability. The proposal would require a data provider to make available to a consumer and an authorized third party, upon request and in a "timely" and "reliable" manner, 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.

— Covered data would be required to be made available in electronic, usable form for consumers and authorized third parties. The data would need to be a machine-readable file that could be retained and transferred into separate information systems.

Covered Data. Under the proposed rule "*covered data*" would mean the most recently updated "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." This would include:

— Transaction information, including historical information (at least 24 months), about individual transactions such as payment amount, date, and payment type.

— Account balance, including available funds in an asset account and any credit card balance.

— Information to initiate payment to or from a Regulation E account.

— Terms and conditions, including APR, annualized percentage yield, fees, and other pricing information.

— Upcoming bill information, including those facilitated through the data provider (e.g., payments scheduled through the data provider or payments due to the data provider).

— Basic account verification information, including name, address, email address, and phone number associated with the covered product or service.

Exceptions to the Obligation. The proposed rule outlines four exceptions that aim to protect sensitive information from being shared or compromised, while still allowing consumers to access essential financial data. These exceptions include:

— Confidential commercial information, including algorithms used to derive credit scores or other risk scores or predictors.

— Information collected by a data provider for preventing fraud or money laundering or detecting and reporting other unlawful conduct.

— Information required to be kept confidential by any other provision of law.

— Information that a data provider cannot retrieve in the ordinary course of its business.

C. Proposed Requirements for Covered Data Access

Proposed Interface Requirements. As proposed, the rule would require a data provider to maintain a consumer interface and to establish and maintain a developer interface through which data providers could receive requests for, and provide, covered data in electronic, usable form to authorized third parties."

The proposed rule would also prohibit data providers from imposing fees or charges for establishing or maintaining the required interfaces, or for receiving requests and making covered data available.

Developer Interfaces. The proposed rule includes additional requirements that would apply specifically to developer interfaces:

— Developer interfaces would be required to provide covered data in a standardized format that follows qualified industry standards to promote compatibility and interoperability.

— Developer interfaces would be required to maintain a "commercially reasonable performance level", with a minimum response rate of 99.5 percent.

— A data provider would be prohibited from "unreasonably restricting the frequency with which it receives and responds to requests for covered data" or "unreasonable access caps". Data providers would be required to ensure that any access restrictions applied are not discriminatory and are consistent for all authorized users.

Data Security. The proposed rule would also require data providers to implement several data security

features in their consumer and developer interfaces, including access credentials and data security programs.

- Data providers would be required to implement data security programs for developer interfaces following the GLBA Safeguards Framework (section 501 of the GLBA or FTC's Standards for Safeguarding Customer Information, as appropriate) to address security risks.
- The proposed rule would allow data providers to "block" or deny a consumer's or third-party's access to interfaces if making covered data available would present significant risk to data security or risk management programs. Examples include denials for lack of information to authenticate a consumer or third-party or around a third-party's data security practices, or if the consumer has revoked the third-party's authorization.

Third-Party Access Requests. Upon request from an authorized third party, a data provider would be required to make covered data available when it receives information "sufficient" to:

- Authenticate the consumer's identity.
- Authenticate the third party's identity.
- Confirm the third party has followed authorization procedures (e.g., copy of signed authorization disclosure).
- Identify the scope of the covered data being requested.

The proposed rule would permit, but not require, a data provider to confirm the authorization and scope of covered data request with the consumer.

Policies and Procedures. The proposed rule would also require data providers to establish and maintain written policies and procedures to comply with the provisions, including:

- Making covered data available and responding to requests.
- Denial of requests for developer interface access.
- Policies and procedures to ensure accuracy.
- Records retention, including data fields made available under the covered data definition and applicable communication methods.

Additionally, the proposed rule would permit data providers to offer revocation methods for third party access to consumer data, provided the revocation methods meet specific requirements, including:

- The revocation methods could not interfere with a consumer's ability to access their covered data.
- They could not materially discourage consumers' or authorized third parties' use of covered data.

D. Proposed Requirements for Authorized Third Parties

Third-Party Authorization Procedures. As proposed, for a third party to become an "authorized third party" it must seek access to covered data from a data provider on behalf of a consumer for the purpose of providing a product or service requested by the consumer. The third party must also:

- Provide an authorization disclosure to the consumer to inform them of key terms of access.
- Certify (in the authorization disclosure) that the third party agrees to certain obligations regarding the consumer's data, including limiting collection, use, and retention of covered data to what is reasonably necessary to provide the requested product or service. *Note*: Under the proposed rule targeted advertising, cross-selling of other products or services, or sale of covered data would not be part of, or reasonably necessary to provide, any other product or service.
- Obtain the consumer's express, informed consent (electronically or in writing) to access covered data on their behalf.

Reauthorization and Revocation. The proposed rule would also:

- Require that third parties obtain new authorization from the consumer to collect, use, or retain covered data beyond a one (1) year maximum period after the consumer's most recent authorization.
- Require that third parties certify to:
  - Providing consumers with easily accessible and operable revocation mechanisms.
  - Notifying the data provider, data aggregator, and certain other third-parties when a consumer revokes authorization.
  - Abiding by certain limitations on collection, use, and retention of covered data when a revocation occurs.

Use of Data Aggregator. The proposed rule would require third party authorization procedures when using a data aggregator to assist with accessing covered data on behalf of a consumer, and would impose certain responsibilities and conditions on third parties and data aggregators:

- Third parties may utilize data aggregators to perform authorization procedures on their behalf but would remain responsible for compliance with rule provisions, including disclosing the use, name, and certification of data aggregators.
- Data aggregators performing the third-party authorization procedures would have to comply with data aggregator certification requirements, including agreeing to conditions on accessing consumer data.

Records Retention. Third parties would be required to establish and maintain policies and procedures designed to ensure retention of records, for a least three (3) years, related to consumer authorizations and compliance with Subpart D of the rule.

Proposed Compliance Dates

Compliance Dates. The proposed rule would provide four (4) tiers of compliance dates, as outlined in the table below:

Tier	Applicable Institutions	Proposed Compliance Date following publication in the Federal Register
1	1) Depository institutions holding at least $500 billion in total assets and 2) non-depository institutions generating at least $10 billion in revenue in the preceding calendar year or are projected to in the current calendar year.	Six (6) months
2	1) Depository institutions holding between $50 and $500 billion in total assets and 2) non-depository institutions generating at less than $10 billion in revenue in the preceding calendar year or project to in the current calendar year.	Twelve (12) months
3	Depository institutions holding between $850 million and $50 billion in total assets.	Thirty (30) months (or 2.5 years)
4	Depository institutions holding less than $850 million in total assets.	Four (4) years

Comment Period

CFPB is seeking public comments on the proposed rule, with a submission deadline of December 29, 2023.

For more information, please contact Amy Matsuo, Todd Semanco, or Chad Polen.

Contact the author:

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com