Updates
November 20, 2024
CFPB Finalizes Proposed Open Banking Rule on Personal Financial Data Rights

Background on Open Banking and the CFPB

The Consumer Financial Protection Bureau (CFPB) recently finalized a rule on personal financial data rights (Rule), implementing Section 1033 of the Consumer Financial Protection Act of 2010 (CFPA). This marks a transformative step toward open banking in the United States. The Rule mandates that certain providers of financial products and services enable consumers' control over accessing and sharing their financial data, promoting increased transparency and competition.

Open banking regulation has been advancing globally, especially in the European Union with the revised Payment Services Directive, which has spurred similar regulatory movements. In the United States, however, open banking has largely been driven by industry practices until now. The CFPB's rule aims to create a more consumer-centric financial ecosystem, allowing consumers greater control over their financial data and offering them the ability to switch providers seamlessly.

For additional background and how this rule interacts with other financial laws and regulations, see our previous Update on open banking and the proposed rule.

Changes From the Proposed Rule

The final Rule includes notable changes from the proposal, such as:

- **Data provider definition.** The Rule makes clear that institutions that merely facilitate first-party payments are *not* considered data providers. So, a merchant or mortgage loan servicer initiating a payment from a consumer's account to itself would not be subject to the data provider requirements of the Rule.

- **Interface specifications.** The Rule elaborates on interface performance metrics, requiring a 99.5% uptime for developer interfaces *per calendar month* and stringent response rate criteria.
- **Anti-evasion provision.** The Rule includes an explicit prohibition against avoiding the Rule's requirements. A data provider must not intentionally evade data access requirements, take actions likely to render covered data unusable, or take actions likely to prevent, interfere with, or discourage access to covered data by consumers or authorized third parties.
- **Fair Credit Reporting Act (FCRA) risk.** In the response to comments about whether data providers are considered furnishers under the FCRA, the CFPB noted that the Rule "does not alter the types of data, parties, or permissible purposes covered by the FCRA" and that the agency "would not consider data providers under this final rule to be furnishers solely by virtue of permitting data access pursuant to an authorization[...] even assuming data are provided to a data aggregator that qualifies as a consumer reporting agency."

Scope of the Rule

Generally, the Rule applies to those entities that are required to provide consumer financial data (data providers), entities seeking to receive consumer financial data (third parties), and consumers seeking to obtain covered data from data providers for themselves and/or in order to provide it to third parties. More specifically, the Rule would apply to the following:

- **Data providers**. The Rule applies to any covered data provider that "controls or possesses covered data concerning a covered consumer financial product or service."
    - Covered data providers include:
        - Financial institutions as defined in Regulation E, such as banks or other entities that directly or indirectly hold a consumer account or issue an access device to provide electronic fund transfer services.
        - Card issuers as defined in Regulation Z, including agents of card issuers but excluding those who only provide services related to the production of cards or processing data for others.
        - Digital wallets, like data providers, fall within this scope and are required to provide consumers or authorized third parties with access to financial data, such as transaction history, account balances, and service terms, while ensuring secure, consent-based data sharing.
    - However, depository institutions that do not have a consumer interface and depository institutions holding total assets less than the Small Business Administration size standard are specifically exempt from the Rule.
- **Covered data**. The Rule applies only to consumers' covered data, which includes transaction information, account balance, payment initiation information, terms and conditions, upcoming bill information, and basic account verification information (*e.g.*, name and email address). Reward program data, such as reward credits and program terms and conditions, are also considered covered data under the Rule.
- **Covered consumer financial products and services**. The products and services subject to the new Rule are asset accounts subject to the Electronic Fund Transfer Act and Regulation E, credit cards subject to the Truth in Lending Act and Regulation Z, and related payment facilitation products and services.
- **Third parties**. Under the Rule, a third party is defined as any person or entity that is not (1) the consumer to whom the covered data pertains or (2) the data provider that controls or possesses the consumer's covered data. This definition encompasses a broad range of entities that may interact with covered data, provided they have obtained the proper authorizations from the consumer. An additional distinction is made for data aggregators, which are persons engaged by an authorized third party to facilitate the processing of covered data.

Key Requirements

Consumer requests. The Rule provides consumers with certain rights to their covered data. Consumers and authorized third parties may make various requests to data providers. Upon authentication, identifying the scope of the request, and documenting the request, data providers are obligated to respond accordingly:

- **Data access**. Upon authentication, a data provider must make consumers' covered data available to them or their authorized third parties in an electronic form usable by the consumer and authorized third parties, provided at no cost.
- **Revocation**. Third parties must provide consumers with the ability to easily revoke their authorization for data access.
- **Exceptions**. Data providers are not required to make available confidential commercial information, such as credit scoring algorithms or data solely used for the purposes of preventing fraud or money laundering. Additionally, data providers may have a practical exception regarding information that is not retrievable in the ordinary course of its business, which is not defined by the Rule.

Data provider obligations. In addition to responding to consumer requests, data providers must also comply with the following:

- **Developer and consumer interfaces**. A data provider must maintain standardized interfaces that meet performance and security criteria—ensuring consistent, user-friendly access for consumers and third-party developers—through which the data provider receives consumer requests.
- **Data provider disclosures**. A data provider must make information readily available as it would be on a public website and in both human-readable and machine-readable formats, including:
    - Data provider identifying information, such as legal name, website link, legal entity identifier, and contact information.
    - Developer interface documentation, including metadata describing all covered data, corresponding data fields, and other documentation sufficient for access and use of the interface.
    - Monthly performance specifications, including a 99.5% uptime requirement for developer interfaces and stringent response rate criteria.
- **Written policies and procedures**. A data provider must establish and maintain written policies and procedures that are reasonably designed to ensure the availability, accuracy, and retention of covered data. These policies must be appropriate to the size, nature, and complexity of the data provider's activities and must be periodically reviewed and updated to ensure their continued effectiveness.
    - *Retention period. Additionally, data providers must retain records of actions taken in response to requests for at least three years, including records of denied access and revocations.*
- **Prohibition on fees**. A data provider is prohibited from charging fees for data access, a move designed to reduce barriers for consumers to switch providers and encourage competitive rates and services.

Third-party obligations. Third parties must obtain the consumer's express informed consent through a signed authorization disclosure to access covered data on behalf of a consumer.

- **Authorization**. The authorization must clearly and conspicuously disclose information about the data provider, product and services, and categories of data accessed.
- **Data use limitation**. Third parties are restricted from using covered data except solely to do what is reasonably necessary to deliver the requested services. The Rule bans any unrelated data collection practices (*e.g.*, for advertising, cross-selling, or selling data). Third parties may still obtain consumer consent for other uses, so long as the consent is presented as consent for a separate product or service.
- **Data collection and duration**. Third parties are limited to collect and process data for up to one year unless reauthorized by the consumer. The CFPB noted that this backstop is to provide consumers additional protection from ongoing data collection where the consumer's needs or expectations may have

changed or where the consumer had intended to revoke a third party's access (*i.e.*, by deleting the mobile application) but did not actually revoke such access.
- **Revocation method**. Third parties must provide an easy method for consumers to revoke authorization without penalties.

Compliance

For certain provisions in the Rule, such as the requirement to create a developer interface, the Rule does not set out strict technical requirements. Instead, covered parties can comply by creating policies and procedures that follow "consensus standards."

Becoming a standards setter. The CFPB finalized the application procedure for organizations to become recognized standard setters this summer and has begun accepting applications for recognition, which would last up to five years, absent revocation.

Application criteria. Standards setters must, at a minimum, meet the following criteria:

- **Openness**. Procedures are open to all interested parties, including consumer groups, financial services experts, authorized third parties, data providers, and relevant trade associations, allowing meaningful, nondiscriminatory participation.
- **Balance**. Decision-making power is balanced across all interested parties, including consumer groups and commercial entities, ensuring no single interest dominates. Representation includes both large and small entities, considering participants' roles and ownership.
- **Due process and appeals**. Documented and publicly available policies ensure adequate notice, time for review, access to views, and a fair process for resolving conflicts, with an appeals process for handling procedural disputes impartially.
- **Consensus**. Standards development proceeds by general agreement, considering comments and objections through fair, impartial, open, and transparent processes.
- **Transparency**. Procedures for participating in and developing standards are transparent and publicly available to all participants.

Guidance and Enforcement

The CFPB has set staggered compliance deadlines based on the institution's size, with the largest providers expected to comply by April 1, 2026, and smaller entities given extended timelines spanning from 2027 to 2030. The rule aligns with existing privacy frameworks like the Gramm-Leach-Bliley Act and mandates that all authorized third parties adhere to data protection requirements. In addition, the CFPB has introduced criteria for the recognition of industry standard-setting bodies, allowing them to support compliance with standardized data-sharing frameworks.

Legal Challenges

On the same day that the finalized rule was released, two banking lobby groups, the Kentucky Banker's Association and the Bank Policy Institute filed a complaint in federal court in Kentucky, alleging that the rule oversteps the CFPB's authority and increases the likelihood of frauds and scams by third parties.

Takeaway

The final rule establishes a significant advancement in consumer financial data rights, potentially reshaping competitive practices across the U.S. financial landscape. By providing consumers with robust control over their financial data, the CFPB's rule could drive better customer service, improved product offerings, and more competitive pricing in the industry.

Implementing data interfaces that meet the rule's high standards of security, accuracy, and availability may require significant infrastructure investments. Organizations will need to prepare for phased implementation and assess how to align data-sharing practices with compliance and technical requirements.

Authors

Explore more in

Financial Transactions Technology Transactions & Privacy Law Fintech & Payments

Related insights

Article

CFPB Issues Proposed Open Banking Rule