Articles
February 29, 2024
CFPB Issues Proposed Open Banking Rule

The Consumer Financial Protection Bureau (CFPB) announced that it was issuing a Notice of Proposed Rulemaking regarding Personal Financial Data Rights on October 19, 2023.

The proposed rule (Proposed Rule) would implement section 1033 of the Consumer Financial Protection Act of 2010 (CFPA), which gives consumers the right to access their financial data and authorizes third parties to access it on their behalf. Data providers would be required to provide consumers and authorized third parties, upon the consumer's request, covered data in an electronic and standardized form consistent with industry standards developed by standard-setting bodies recognized by the CFPB. Additionally, the rule would limit authorized third parties' collection, use, and retention of covered data.

While the Proposed Rule would pave the path for new industry standards and facilitate adoption of open banking, companies should be mindful of the rule's legal and regulatory implications under existing laws, such as the Fair Credit Reporting Act (FCRA), the Electronic Fund Transfer Act (EFTA), and the Gramm-Leach-Bliley Act (GLBA).

What Is Open Banking?

Open banking refers to the practice of allowing consumers to access and share their financial data from different financial institutions through secure digital platforms, such as application programming interfaces (APIs), to increase competition, innovation, and transparency in the financial sector. Open banking could, for example, allow a consumer to share their transaction history from one financial institution to support their application for a loan at another financial institution. Open banking also could provide a means for a consumer to aggregate all of their financial data in one centralized dashboard for easy review.

Historically, in order for third-party providers (TPPs) to offer consumers services related to their financial data, the TPPs used practices such as "screen scraping," the process by which a consumer provides the TPP login credentials in order for the TPP to collect the data via automated scraping code. In some cases, screen scraping presents heightened security risks and errors in transaction processing, in addition to raising concerns about the ability of financial institutions to protect their systems from unwanted uses. As technology advanced, industries sought to create more secure and accurate methods to collect such information, resulting in open banking APIs.

To facilitate the development of open banking, jurisdictions around the world have implemented relevant laws and technical standards. The European Union has been at the forefront of developing a legal framework for open banking. The Payment Services Directive (PSD) laid the foundation, followed by the Revised Payment Services Directive (PSD2). PSD2 brought several changes, such as enhanced consumer protection, stricter security measures (i.e., prohibiting screen scraping), and mandatory data access for TPPs upon customer consent.

Notice of Proposed Rulemaking

While development of open banking in the United States has been largely industry-driven, the CFPB's Proposed Rule regarding Personal Financial Data Rights would create the country's first federal legal framework for open banking.

Scope

Generally, the Proposed Rule would apply to the following:

- **Data providers.** The Proposed Rule would apply to any data provider that "controls or possesses covered data concerning a covered consumer financial product or service," except for depository institutions that do not have a consumer interface.
- **Covered consumer financial products and services.** The products and services subject to the new rule are asset accounts subject to the EFTA and Regulation E, credit cards subject to the Truth in Lending Act (TILA) and Regulation Z, and related payment facilitation products and services.
- **Covered data.** The Proposed Rule applies only to 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). Covered data does not include, for example, "algorithm[s] used to derive credit scores or other risk scores or predictors" or information collected solely to prevent money laundering.

  Obligations

  Primarily, the Proposed Rule would require data providers to make available to a consumer or 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 would have to be provided in an electronic form usable by consumers and authorized third parties.
- **Identity verification.** The Proposed Rule would require that covered entities authenticate the consumer's (and, where applicable, the third party's) identity before disclosing the requested data.
- **Data format.** In providing the requested data, covered entities would be required to use a machine-readable file format that can be retained and controlled by the consumer or authorized third party for processing in a separate system.

- **Interfaces.** Following industry standards, the data provider would be required to create a developer interface and maintain both the developer and consumer interfaces. In addition to satisfying data requests, data providers would also have to maintain commercially reasonable performance, including a service level of at least 99.5% uptime, not including scheduled downtime.
- **No fees.** The data provider would be prohibited from charging fees to a consumer or an authorized third party for maintaining the interfaces or satisfying the requests.
- **Accuracy.** Data providers would also be required to establish and maintain policies and procedures reasonably designed to ensure accuracy of covered data made available through its developer interface.
- **Privacy and data security.** The Proposed Rule would also require that covered entities and TPPs ensure certain privacy and security measures are in place, including where required by the GLBA. Access, collection, use, and retention of covered data on behalf of a consumer is generally limited to only what is reasonably necessary. The Proposed Rule makes clear that the sale or use of data for targeted advertising is not reasonably necessary. Certain written disclosure would be required to be given to the consumer, and the consumer would need to provide written consent for a data provider to fulfill a data request from a third party.

- **Informed authorization.** Third parties would be required to ensure that consumers are informed of the third party's access to their covered data by providing them with a copy of the authorization disclosure, contact information, and, upon request, information about the categories, reasons, parties, status, and revocation of the third party's access to their covered data. The third party would need to provide the consumer with a mechanism to revoke the third party's authorization to access their covered data that is as easy to access and operate as the initial authorization.

Timeframe

The Proposed Rule would establish different compliance dates, ranging from six months to four years from the date of the final rule, for data providers based on their size and type.

Potential Areas of Risk

The CFPB's notice makes clear that the new rule does not eliminate the requirements of other laws. Accordingly, data providers and third parties should carefully consider new legal and regulatory risks posed by open banking regimes, including the following.

Fair Credit Reporting Act. The FCRA is a federal law that regulates the collection, use, and disclosure of so-called "consumer report" information by consumer reporting agencies (CRAs), users of consumer reports, and furnishers of information to CRAs. With increased data mobility and access resulting from open banking, entities could potentially consider consumers' eligibility for credit, insurance, or employment in novel ways using new data points not traditionally included in consumer reports today (e.g., transaction history).

Depending on the specific use case, communication of these new data points for this purpose could potentially trigger the FCRA's definition of "consumer report" information. This could render third-party providers and other open banking participants subject to various FCRA compliance requirements.

Electronic Fund Transfer Act. The EFTA provides consumer protection and disclosure requirements for electronic fund transfers (EFTs), such as debit card transactions, ATM withdrawals, direct deposits, and preauthorized transfers. Covered entities, such as financial institutions, merchants, and service providers, may face liability under the EFTA for various violations, including for unauthorized EFTs.

With the development of open banking, entities subject to the EFTA may face new issues in determining whether the consumer has authorized a particular EFT. For example, the accessibility and ease of use associated with APIs could potentially give rise to unauthorized users initiating unauthorized transfers.

Gramm-Leach-Bliley Act. The GLBA and its implementing regulations require financial institutions and certain other entities that collect, use, or share nonpublic personal information (NPI) of consumers and customers to protect the privacy and security of such information and to provide notice and opt-out rights about certain data practices. Companies working to comply with the CFPB's open banking rule must keep these requirements in mind as they respond to and comply with consumer data requests. This includes implementing appropriate security measures to mitigate the risk of unauthorized third parties from wrongfully obtaining customer data.

Conclusion

The CFPB's Proposed Rule regarding Personal Financial Data Rights marks a significant step toward open banking in the United States. This innovative approach promises to empower consumers with control over their financial data and to foster competition in the industry. However, although the Proposed Rule paves the way for an open banking future, stakeholders will need to collaborate to address legal uncertainties and establish strong privacy and security frameworks. Addressing the uncertainties surrounding the FCRA, EFTA, and GLBA within the Proposed Rule's framework will be essential for a successful and responsible implementation of open banking.

Authors

Explore more in

Financial Transactions | Privacy & Security | Technology Transactions & Privacy Law | Fintech & Payments | Financial Services & Investments | Digital Media & Entertainment, Gaming & Sports