CFPB Pushes Move to an Open Banking System with the Personal Financial Data Rights Rule and Sparks Immediate Court Challenges from Industry

Matthew C. Luzadder, Donnelly L. McDowell, Alexander I. Schneider

October 24, 2024

On Tuesday, the Consumer Financial Protection Bureau (CFPB) released the final version of the Personal Financial Data Rights Rule that requires many financial institutions, credit card issuers, and other financial service providers that facilitate payments (including mobile wallets and payment apps) to support new open banking standards and make account records accessible and portable. The CFPB uses the term "open banking" to refer to the ability of customers to share personal financial data between a network of entities.

The Rule's Coverage

Section 1033 of the Dodd-Frank Act provides that covered entities must make available to a consumer, upon request, specified information in their control related to consumer financial products or services. Congress also authorized the CFPB to "prescribe standards applicable to covered persons to promote the development and use of standardized formats for information," with the stated goal of increasing competition and encouraging innovation by requiring that covered entities make available to a consumer, upon request, information related to a consumer financial product or service. The rule implements Section 1033 by requiring covered banks, credit card issuers, and certain financial service providers – collectively called "data providers" – to enable consumers to give third parties access to transaction information, account balance information, ACH details, account terms and conditions, bill information, and basic account verification information. The information must be made available in an electronic form usable by consumers or authorized third parties. The final rule is limited to account records regarding "covered financial products and services," which are bank debit accounts (i.e., Regulation E-covered accounts), credit card accounts (i.e., Regulation Z accounts), or the facilitation of payments from such accounts.

What's Not Covered

Covered data providers are not required to disclose confidential commercial information, such as algorithms to derive credit scores or risk predictors; information used for preventing fraud, money laundering, or reporting potentially unlawful conduct; or any information that the data provider cannot retrieve in the ordinary course of business. However, the rule makes clear that a data

provider cannot restrict access to financial information simply because it is subject to privacy protections.

Third Party Collection and Use Restrictions

The rule also establishes obligations for the third parties accessing consumers' data. For example, third parties must limit the collection, use, and retention of covered data to what is reasonably necessary to provide the product or service requested from the third party by the consumer. The CFPB makes clear that it does not consider third party use of open banking data for targeted advertising, cross-selling, or the sale of the data to be permitted under the regulations. Third parties also face limitations on their access to covered data. Access is limited to one year without reauthorization, and consumers must be provided with the ability to immediately revoke access resulting in the deletion of their data upon request.

Standards Instead of Web Scraping

According to the Bureau and the rulemaking record, the rule seeks to move the financial services industry away from the "screen scraping" approach relied upon by many businesses, which typically involves consumers providing their account passwords to third parties who use them to access and copy data through online banking portals. The final rule shifts towards open banking through a standardization of third party data access. Instead of scraping data from customer accounts, data providers will be required to establish developer interfaces for third parties to access the customers' financial data. The rule includes requirements for these interfaces that promote standardized operations, including minimum performance requirements, and security measures, including a requirement to implement an information security program applicable to the interface.

Legal Challenges

Certain industry groups immediately pushed back against the rule by filing a court challenge in the U.S. District Court for the Eastern District of Kentucky, arguing that the rule exceeds the Bureau's Section 1033 authority and is arbitrary and capricious under the Administrative Procedure Act.

If the rule withstands legal challenges, larger providers would be required to comply with it by April 2026, while the smallest covered institutions would have until April 1, 2030. Certain small banks and credit unions would be exempt altogether. We'll continue to follow the pending litigation closely.