CFPB'S 1033 OPEN BANKING RULE

Final Rule and Developments Since its Publication

Grayson LaMontagne of Poyner Spruill LLP and **Nick Christopherson**

The increasing number of financial products and services in the market has created new challenges for consumers and regulators in the financial industry. Consumers want their data protected, but they also expect seamless integration between different financial service platforms. For these reasons, the Consumer Financial Protection Bureau ("CFPB") published its Personal Financial Data Rights Rule, commonly referred to as the "Open Banking Rule" (the "Rule"), in late 2024 to "give consumers greater rights, privacy, and security over their personal financial data."[1] The Rule requires financial institutions, credit card issuers, and other financial providers to unlock consumers' personal financial data and transfer it to another provider upon request for free, moving the United States closer to having an open banking system similar to the United Kingdom and European Union.

The Rule has been years in the making, dating back to 2010, when Congress passed the Dodd-Frank Wall Street Reform and Consumer Protection Act, which established the CFPB and provided the authority for the Rule under Section 1033. In 2017, the CFPB first issued a Request for Information on the subject and issued an Advance Notice of Proposed Rulemaking in 2020. The final Rule was published in late 2024 and immediately became embroiled in trade-group litigation and political turmoil, which have threatened to undo years of work and progress. Nevertheless, despite the Rule's uncertain future, financial institutions and fintechs should understand the key compliance issues surrounding the Rule's implementation to best protect themselves against the range of possible outcomes.

FINAL RULE AND KEY COMPLIANCE ISSUES

Covered Entities

The Rule requires "data providers" to make "covered data" related to "covered financial products and services" available to consumers and "authorized third parties" without charge.[2] "Data providers" means any person (or affiliate that acts as a service provider) that engages in offering or providing a consumer financial product or service and who is (i) a financial institution (as defined in Regulation E), (ii) a card issuer (as defined in Regulation Z) or (iii) any other person that controls or possess information concerning a covered consumer financial product or service that the consumer obtained from that person. This definition includes depository institutions (including credit unions) and non-depository institutions that issue credit cards, hold transaction accounts, issue devices to

access an account, or provide other types of payment facilitation products or services. This definition also covers many types of fintechs.

"Covered data" includes information about transactions, costs, charges, and usage, such as account balance, payment-initiation data, terms and conditions, upcoming bill information, and basic account verification information. Covered data does not include, however, confidential commercial information (e.g., credit score algorithms), information collected to prevent fraud or money laundering or to detect illegal conduct, information required by law to remain confidential, and information that is not retrievable in the ordinary course of business.

"Authorized third parties" means a third party that has complied with certain authorization procedures that include (i) providing a consumer with an authorization disclosure, (ii) certifying and agreeing to limit its collection of covered data to what is reasonably necessary to provide the consumer's requested product or service and agreeing to not use the covered data for targeted advertising, cross-selling other products or services, or selling the covered data, and (iii) obtaining the consumer's express informed consent to access the covered data on behalf of the consumer.

Key Obligations

a. Free Access. The Rule requires data providers to create two interfaces for handling data requests. One for consumers and one for authorized third parties and their "data aggregators" (persons that access covered data for and on behalf of authorized third parties). Importantly, data providers must not allow third parties to access the developer interface with the same credentials that a consumer uses to access the consumer interface. In both interfaces, data providers must grant consumers, authorized third parties, and data aggregators access to covered data in electronic form, and in a manner that is usable by the consumer and authorized third party. In addition, the Rule prohibits data providers from charging fees for establishing or maintaining the interfaces or for processing requests for covered data.

Developer interfaces require additional requirements beyond those required for consumer interfaces, which include providing covered data in a "standardized format" with "commercially reasonable performance." "Standardized format" means a manner that conforms to a format widely used by other data providers and designed to be readily usable by authorized third parties. "Commercially reasonable performance" requires demonstration of several compliance indicia, but the most notable requires that the interface processes requests with 99.5% accuracy.

b. Written Policies; Reporting. The Rule obligates data providers to maintain written policies that are "reasonably designed" to achieve the objectives of the Rule, including making covered data available, ensuring accuracy in the processing of requests, and retaining certain transaction records to demonstrate compliance with the Rule. In addition, the Rule requires data providers to disclose certain information about the data provider (such as its legal name, a link to its website, contact information, developer interface documentation, and performance disclosures) in a manner "at least as available as it would be on a public website."

Enforcement Timeline

The Rule will be implemented in phases, affecting bigger institutions as early as April 1, 2026, and smaller ones as late as April 1, 2030. Specifically, the Rule requires compliance for the following entities prior to the dates set forth below:

April 1, 2026

Depository Institutions. Total assets equal to or greater than $250 billion.
Non-Depository Institutions. Total receipts as of 2023 or 2024 equal to or greater than $10 billion.

April 1, 2027

Depository Institutions. Total assets equal to or greater than $10 billion, but less than $250 billion.
Non-Depository Institutions. Total receipts as of 2023 or 2024 less than $10 billion.

April 1, 2028

Depository Institutions. Total assets equal to or greater than $3 billion, but less than $10 billion.

April 1, 2029

Depository Institutions. Total assets greater than $1.5 billion, but less than $3 billion

April 1, 2030

Depository Institutions. Total assets equal to or greater than $850 million, but less than $1.5 billion.
Depository institutions with total assets below $850 million are exempt from the Rule.

LEGAL CHALLENGES AND PREDICTIONS FOR THE FUTURE OF OPEN BANKING

The Rule has faced significant scrutiny from lenders and banking groups who argued that the open banking framework imposed by the CFPB would put consumer information at risk and burden financial institutions with substantial costs. The Kentucky Bankers Association and the Bank Policy Institute filed a lawsuit against the CFPB, asserting that the agency was "overstepping its statutory mandate and injecting itself into a developing, well-functioning ecosystem," in which banks, their regulators and fintech companies worked together to seamlessly and safely integrate open banking practices using their expertise.

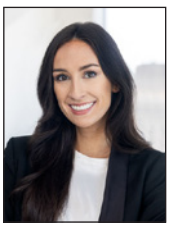
In light of this lawsuit, CFPB leadership reviewed the Rule and agreed that the current framework exceeds the authority conferred to the CFPB by Section 1033. Namely, Section 1033 does not authorize broad regulation in the form contemplated and also does not authorize the CFPB to prohibit banks from charging any fees. The CFPB responded with a motion for summary judgment and requested that the court find the Rule unlawful. The CFPB has since worked to rescind the Rule along with a bevy of other rules that exceed its statutory authority.

With the withdrawal of the Rule, the CFPB will be forced to rework its open banking concept to prescribe a standardized format and standards to support the goals of open banking. Section 1033, as the authority for the Rule, still requires that the CFPB promulgate a rule that allows consumers access to "transaction data" and "information concerning a consumer financial product or service." However, with a new administration in office and defunding of the CFPB, there is uncertainty surrounding how Section 1033 will be implemented going forward. Although banks and financial institutions have already made strides towards "open banking" by implementing mechanisms for consumers to access and share their data, the practice is largely unstandardized until new authority is put in place.

---

[1] *CFPB Finalizes Personal Financial Data Rights Rule to Boost Competition, Protect Privacy, and Give Families More Choice in Financial Services, CFPB Newsroom* (Oct. 22, 2024), https://www.consumerfinance.gov/about-us/newsroom/cfpb-finalizes-personal-financial-data-rights-rule-to-boost-competition-protect-privacy-and-give-families-more-choice-in-financial-services/.

[2] 89 Fed. Reg. 90839 (Nov. 18, 2024).



Grayson LaMontagne works with clients on a variety of commercial loan transactions. She represents borrowers, lenders, and financial institutions in a wide range of transactional matters. Grayson is an associate attorney at Poyner Spruill LLP.