Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

September 30, 2025

Access to Consumer Financial Data: Open Banking and the CFPB's Section 1033 Rule

Open banking refers to a relationship among consumers, financial services providers, and authorized third parties that enables consumers to transfer their information electronically from one firm to another for varied purposes. Motivations for open banking include making it easier to move financial accounts between providers and enabling free flow of information to novel applications. However, the degree to which adoption of open banking should be market-driven by industry due to consumer demand or regulation-led is debated. Open banking also relates to a broader policy issue regarding ownership of data and the degree to which data should belong to a consumer or to the financial institution.

Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (P.L. 111-203) requires covered financial institutions to make available to consumers upon request certain data associated with their accounts, subject to rules prescribed by the Consumer Financial Protection Bureau (CFPB). The CFPB finalized a rule in October 2024, with implementation originally set to begin in April 2026. Currently, the rule is the subject of litigation and reconsideration by new CFPB leadership.

Background

In practice, open banking consumer-permissioned data transfers originate from data providers, often the depository institutions where consumer hold their primary accounts, generally through data aggregators that verify the information and connect it to authorized third parties. For example, a consumer with a checking account, investment account, and credit card account at three separate financial institutions may authorize a financial technology (fintech) app provider to show the accounts' balances on one interface for budgeting purposes. Examples of these firms that could act as data providers or authorized third parties include depository institutions or nonbanks such as payment platforms, budgeting applications, or crypto firms. Financial institutions that are primarily data providers, data aggregators, or authorized third parties may have different policy motivations for this policy issue.

Data sharing platforms in financial services are common in the United States, with previous estimates finding that, as of 2024, at least 100 million consumers authorized third parties to access their financial data. Among other things, the Gramm-Leach-Bliley Act (GLBA, P.L. 106-102) regulates the disclosure and safeguard of non-public information in the financial sector. GLBA generally prohibits financial institutions from disclosing non-public information to non-affiliated third parties without providing consumers notice and a reasonable ability to opt out of such disclosures. One exception to GLBA is that consumers may consent to or direct such disclosures, hence enabling the current system of data sharing. Data sharing often uses application programming interfaces (APIs) or sometimes (and more controversially) screen scraping to facilitate information sharing without the need for manual input. *Screen scraping* refers to a consumer providing his or her account credentials and permission to a third party to "scrape" the account and activity information from a financial institution's user interface. Scraping enables the transfer of data, although such practices may present added data security and privacy risks. API connections are most common at the larger banks, and smaller banks may face challenges in setting up these platforms, as creating and maintaining these connections may be relatively costlier for smaller institutions and impose additional risks. Financial institutions of different varieties and sizes have differing interests related to consumer financial data, its access, who pays for sharing, what types of data are shared, and compliance with scam-related or data-privacy-related statutes that correspond with such sharing.

Section 1033 of Dodd-Frank and the CFPB Rule

Though a rule implementing Section 1033 was not finalized until 2024 and is currently set to be implemented over the course of the next several years, Certain financial firms had already begun offering open banking services, before the finalized rule, driven by anticipated regulatory action and/or consumer demand for such services. Regulatory standards that mandate open banking are fairly common in European countries, although their specific rules may differ from the final rule of Section 1033.

As discussed in greater detail below, this rule is currently the subject of litigation and reconsideration by new leadership at the CFPB. In short, the final rule says the following:

- Covered entities, such as depository institutions with $850 million or more in assets and certain nonbanks, must make certain data available to consumers and authorized third parties in an electronic form.
- Covered financial data include transactions from the past 24 months, terms and conditions associated with the account, and personal account information.
- The rule was set to take effect starting January 2025. The original implementation timeline varied based on institution size and meant that the largest bank and nonbank data providers would have had to comply in April 2026. The smallest depository institutions covered

by this rule would have had to comply by April 2030. These compliance dates have been stayed for 90 days.

- The rule imposes certain disclosure obligations on authorized third parties, limits the use of covered data to the requested product or service, limits the collection of data to one year, and requires that third parties comply with data security rules under GLBA.
- The rule bans financial institutions from levying fees or charges on consumers or third parties for data transfers.
- The rule limits third party use of consumer financial data to that which is "reasonably necessary to provide the consumer's requested product or service."
- The rule defined consumers who could transfer data as "natural persons" and those acting on their behalf (guardians, trustees, or custodians).

There is no novel distribution of liability outlined in this rule. As a result, any financial institution liability from scams and fraud would likely be driven by existing standards outlined in Regulations E and Z.

Response to the Rule

The reaction to the final rule was mixed. Fintechs generally favored the final rule, while banks generally opposed the version finalized by the CFPB. These differing views reflect the broader fintech-bank dynamic characterized by competition for customers and the provision of services and distinct regulatory frameworks. This competition is often reflected in different policy motivations and preferences for fintechs and banks on certain issues, including the Section 1033 rulemaking.

Some hailed the rule as a step toward enshrining new data privacy protections, promoting consumer choice, fostering competition, and driving innovation. Others argued that the rule was "central planning dressed up as consumer choice," lacked clear rules for liability, and had security and oversight gaps. The same day that the rule was finalized, Forcht Bank, the Bank Policy Institute, and the Kentucky Bankers Association brought a lawsuit against the CFPB arguing that the final rule overstepped its statutory authority.

Recent Market and Regulatory Developments

In May 2025, the Financial Technology Association, a fintech industry group, was granted the right to intervene in this lawsuit defending the rule. Shortly following this development, the chief legal officer of the CFPB, Mark Paoletta, filed a motion in the lawsuit to withdraw the rule, noting that under new leadership the CFPB considered the rule to be "unlawful and should be set aside."

With the uncertainty surrounding the finalized Section 1033 rule, some depository institutions have suggested that they may start charging data aggregators or third parties for this data. Specifically, JPMorgan Chase (JPMC) had reportedly indicated to data aggregators that they would begin charging fees for fintechs to access their data, with the highest fees for payments-focused companies. In part, this desire stemmed from the supposed volume of API calls that were associated not with *individually* consumer-permissioned requests, but with initial permissions granted once at account opening. This reflects an argument in the recent lawsuit that disagreed with the CFPB banning fees for data transfers. In September 2025, JPMC and Plaid announced a new data transfer agreement that "includes a pricing structure." The specifics of the deal were not publicly announced. The press release with JPMC and Plaid stated that the companies' agreement would not impact Plaid's current customer agreements and pricing. The degree to which this agreement will be an anchor to potentially impact the future Section 1033 reconsideration or future potential agreements between data aggregators and providers is an open question. According to the CFPB rule, data providers do incur one-time and variable costs in creating APIs that comply with relevant data security laws.

The Financial Technology Association, the American Fintech Council (another fintech industry group), and Andreessen Horowitz—a prominent firm invested in cryptocurrency and fintech—have argued various points, including that these charges as agreed to by JPMC and Plaid are prohibited under current statute and could adversely affect the flow of consumer financial data, negatively impacting competition and choice. Others—such as the Bank Policy Institute, Consumer Bankers Association, and American Bankers Association—have argued that data aggregators paying for data helps cover banks' business expenses associated with sharing consumer data, asserted that charging for API access is common in other industries, and pushed for a reconsidered rule that they argue better "comports with the statute."

One concern raised by JPMC and the Bank Policy Institute during the Section 1033 rulemaking was that this rule could facilitate increased payments directly from bank accounts that may have comparatively fewer consumer protections relative to card transactions. These card transactions are profitable for JPMC and other banks—garnering fees from credit cards and interchange from debit cards—relative to payments directly from checking or savings accounts. The reportedly higher fees for payment platforms from JPMC may indicate a specific desire to stem payment-based transfers. Among both regulation-led and market-driven approaches in other countries, payments information was the most common data type that could be exchanged.

In response to these market developments and in contrast to the initial announcement to withdraw the rule, in July 2025, the CFPB filed a motion that it now plans to engage in an "accelerated rulemaking" that would "substantially revise" the rule. In response to this development, the lawsuit is currently stayed pending the new rulemaking. In August 2025, the CFPB issued an Advanced Notice of Proposed Rulemaking outlining 36 questions related to the original rule covering information security and privacy, the ban on fees or charges, and the definition of *consumer*.

Karl E. Schneider, Analyst in Financial Economics

IF13117

Disclaimer