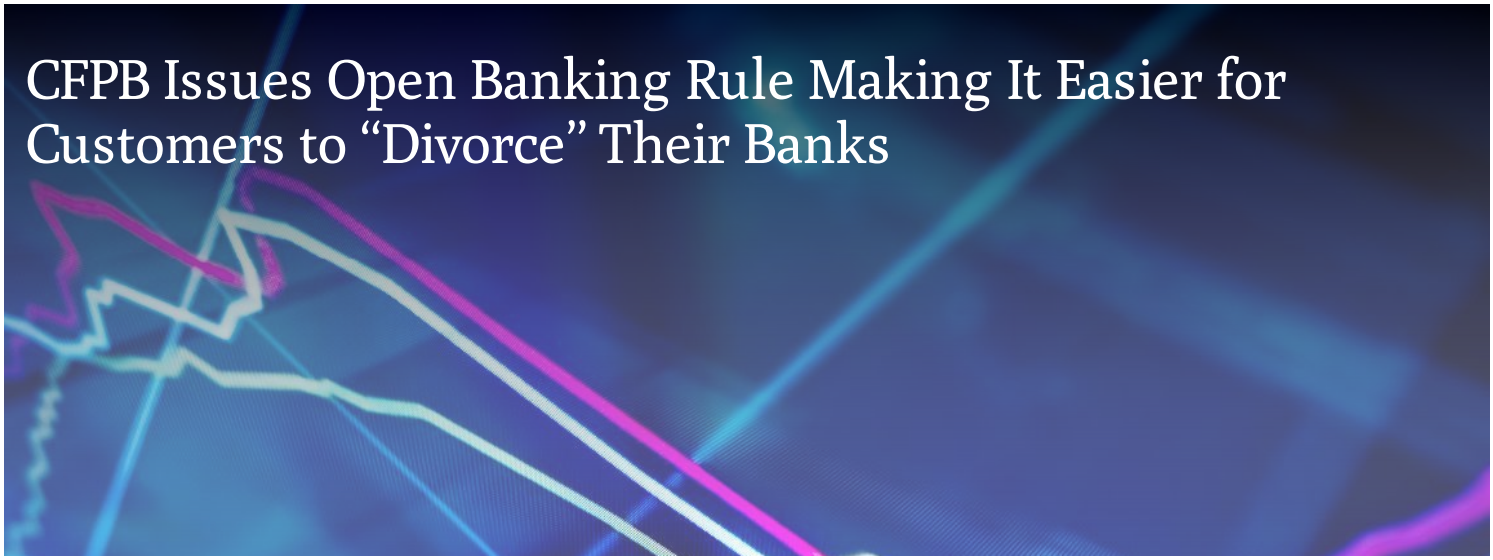
WINSTON & STRAWN LLP

CLIENT ALERT

CFPB Issues Open Banking Rule Making It Easier for Customers to "Divorce" Their Banks



DECEMBER 5, 2024

On October 22, 2024, the Consumer Financial Protection Bureau (CFPB) issued a final rule to enforce consumers' personal financial data access rights granted to them by Section 1033 of the Consumer Financial Protection Act (CFPA), 12 U.S.C. § 5553 (the Rule). Commonly referred to as the "open banking" rule, the Rule is intended to offer consumers the ability to easily switch between providers of financial services and products, increase innovation and greater quality in services, and create baseline security standards for sharing and accessing information across the market.

In sum, the Rule requires data providers (consisting of both depository institutions and nondepository financial institutions, such as credit card issuers) to, upon request, make available to consumers and authorized third parties, in an electronic, reliable, and secure manner, covered data within the data providers' possession or control regarding covered consumer financial products and services that the consumer obtained from the data provider, subject to certain exceptions. The Rule additionally imposes obligations on authorized third parties that obtain covered data from data providers.

Data providers subject to the Rule will need to maintain a consumer interface and developer interface and, subject to certain exceptions, be able to make available covered data in a machine-readable file that can be retained and transferred for processing in a separate information system. In addition, data providers will need to establish and maintain written policies and procedures, commensurate with the size, nature, and complexity of the data provider's activities, that enable the provider to meet the objectives of the Rule.

REACTIONS TO THE RULE

Almost immediately after the Rule was finalized, the Bank Policy Institute and the Kentucky Bankers Association filed a lawsuit against the CFPB, alleging that, among other things, (i) the Rule far exceeds the scope of its statutory authority under Section 1033 of the CFPA (using as an example that Section 1033 only requires data providers to provide covered data to consumers, agents, trustees, or representatives, not to the wide swath of parties that could fall within the ambit of "authorized third parties"); (ii) the Rule is "arbitrary, capricious, an abuse of discretion or not otherwise in accordance with law" under the Administrative Procedure Act ("APA") because it unreasonably requires data providers to share customers' most sensitive financial information, limiting their ability to protect their consumers (and contradicting requirements of the Interagency Guidance on Third Party Relationships: Risk

Management issued by the prudential regulators in June 2023); and (iii) the time frame for compliance with the Rule is fundamentally irrational in violation of the APA.

The plaintiffs additionally argue that open banking has achieved significant progress within the United States through the private sector, without regulatory interference, and that by finalizing a Rule substantially similar to the proposed version of the Rule, the CFPB ignored many of the thousands of comments it received requesting substantial changes to the proposal. According to the various pleadings in the case (including amended complaints filed by the plaintiffs on November 26, 2024), the CFPB has until January to respond to the complaint.

FUTURE OF THE RULE

It remains to be seen what impact the transition of the U.S. presidential administration and congressional branches approaching in January 2025 will have on the Rule. Theoretically, the transition could result in the Rule being rescinded, scaled back, or otherwise modified, its effective date delayed, and/or impact the CFPB's position in the above case. Notably, the Congressional Review Act ("CRA"), codified at 5 U.S.C. §§ 801–808, provides Congress with special procedures—via joint resolution of disapproval introduced during a continuous session period of sixty (60) days starting from the date that the rule has been published in the Federal Register and received by Congress—under which to consider legislation to overturn certain federal rules. The sixty (60)-day period includes every calendar day, including weekends and holidays, and excludes only days that either chamber (or both) is adjourned for more than three (3) days following an adjournment resolution. If a CRA joint resolution of disapproval is timely filed and approved by both houses of Congress and signed by the President, or if Congress overrides a presidential veto, the rule at issue cannot go into effect or remain in effect. Because the Rule was published in the Federal Register on November 18, 2024, there will presumably still be time for a joint resolution of disapproval to be filed once new members of Congress are sworn into office.

However, we note that the proposed rule was met with bipartisan support (reducing the likelihood of the filing of a joint resolution of disapproval), and that the Rule brings the United States more closely in alignment with global open banking practices, such as those of the United Kingdom and European Union. While there are several potential drawbacks associated with open banking that should not be discounted (such as the cost and resources required for data providers to comply with the Rule and the challenges to maintain data security) open banking addresses significant bipartisan policy issues such as innovation and optimization in payment processes and the potential for customer personalization. For those reasons, it is possible, if not likely, that the CFPB open banking rule is here to stay.

Below is a description of the key provisions of the Rule.

KEY DEFINITIONS

As defined by the Rule:

A "*data provider*" is "a covered person" (as that term is defined by 12 U.S.C. § 5481(6)), that is: a financial institution under Regulation E (12 C.F.R. § 1005.2); a card issuer under Regulation Z (12 C.F.R. § 1026.2); or any other person that controls or possesses information concerning a "covered consumer financial product or service" that the consumer obtained from that provider. The term includes both depository and nondepository institutions, with an exclusion for certain small depository institutions.

A "*covered consumer financial product or service*" is a consumer financial product or service as defined by 12 U.S.C. § 5481(5), that is an account under Regulation E (a "Regulation E Account"); a "credit card" as defined under Regulation Z (a "Regulation Z Credit Card"); or the facilitation of payments from a Regulation E Account or a Regulation Z Credit Card, excluding products or services facilitating first-party payments initiated by the payee or an agent of the payee.

"*Covered data*" refers to, as applicable:

- transaction data (e.g., payment type, transaction date, pending or authorized status, payee name, rewards, credits, finance charges, and at least twenty-four (24) months of historical transaction data, if applicable);

- account balance information;
- terms and conditions of the legal agreements between data providers and consumers, including the fee schedule, annal percentage rate or annual percentage yield, credit limit, a consumer's opt into overdraft coverage, etc.;
- upcoming bill payments (which, as an example, include information about third-party bill payments scheduled through a data provider, and any upcoming payments due from the consumer to the data provider);
- basic account verification information (and, if applicable, a truncated account number); and
- information to initiate payment to or from a Regulation E Account directly or indirectly held by the data provider, including account number (tokenized or non-tokenized) and routing number for ACH transactions.

Exceptions to Covered Data: Covered data does *not* include (i) confidential commercial information, such as algorithms to develop credit or risk scores; (ii) information collected by a data provider for the sole purpose of deterring fraud or money laundering, or detecting, or making any report regarding, other unlawful or potentially unlawful conduct; (iii) any information required to be kept confidential by any other provision of law; or (iv) any information that the data provider cannot retrieve in its ordinary course of business.

PROVISION OF INFORMATION

To comply with the Rule, a data provider is required to make available the most recently updated covered data that it has in its possession or control at the time of the consumer's or authorized third party's request, including transactions that have been authorized but not yet settled. In addition, a data provider must ensure that, prior to providing covered data in response to a request from a consumer, it receives information sufficient to authenticate the identity of the consumer making the request, and identify the scope of data requested. If the request is received from a third party, the data provider must perform those same measures, in addition to authenticating the third party's identity, and documenting that the third party has followed authorization procedures set forth in Section 1033.401 of the Rule.

The Rule prohibits a data provider from taking any action with the intent of evading the requirements of the Rule, rendering data that it makes available unusable, materially interfering with a consumer's or authorized third party's access to covered data, or charging fees in connection with requests for data from consumers or authorized third parties or from maintaining interfaces (described below) to provide the data. Nonetheless, a data provider can deny consumers or third parties access to information if (i) providing the information would be inconsistent with the data provider's policies and procedures that are reasonably designed to meet the safety and soundness standards of a prudential regulator, information security standards required by Section 501 of the Gramm-Leach-Bliley Act ("GLBA"), or other applicable laws and regulations regarding risk management; and (ii) the denial is "reasonable" (measured by the indicia for "reasonableness" provided within the Rule).

In addition, a data provider is not required to provide covered data under certain circumstances, such as if the data is not within the data provider's control, the third party requesting covered data is no longer authorized, or the requested information falls within an exception to "covered data" (identified above).

INTERFACE REQUIREMENTS

The Rule requires data providers to maintain a consumer interface and developer interface and, subject to certain exceptions, be able to make available covered data in a machine-readable file that can be retained and transferred for processing in a separate information system. Pursuant to the Rule, the CFPB requires a developer interface's performance to be commercially reasonable, and to make available covered data in a machine-readable and standardized format.

To be considered "commercially reasonable," the response rate must be greater than or equal to 99.5% in a calendar month, excluding scheduled downtime. To qualify as a proper "response" during unscheduled downtime, the response must fulfill the request, or explain why the request could not be fulfilled, be consistent with the data provider's reasonable written policies and procedures established in accordance with the Rule, and be provided

within a commercially reasonable amount of time that conforms to an applicable consensus standard. The Rule provides indicia to measure compliance with each of the foregoing, and sets forth performance specifications.

The Rule prohibits data providers from unreasonably restricting the developer interface frequency with which they receive or respond to requests for covered data from an authorized third party, noting that frequency restrictions must be applied in a nondiscriminatory manner and in compliance with the data provider's reasonable written policies and procedures that it establishes and maintains under the Rule.

Finally, the Rule prescribes security specifications for the developer interface, imposing restrictions related to access credentials and requiring that the developer interface comply with the GLBA or the Federal Trade Commission's ("FTC") Standards for Safeguarding Customer Information (16 C.F.R. Part 314), as applicable.

POLICIES AND PROCEDURES

A data provider is required to establish and maintain written policies and procedures, commensurate with the size, nature, and complexity of the data provider's activities, that enable the provider to meet the objectives of the Rule. Such policies and procedures must cover (i) making covered data available; (ii) ensuring the accuracy of covered data provided through the developer interface; and (iii) record retention.

EXCLUSIONS TO THE RULE

Small depository institutions with assets equal to or less than the "Small Business Administration (SBA) size standard" are excluded from coverage by the Rule, *unless* such depository institutions hold total assets greater than the SBA size standard as of or at any point within sixty (60) days after the publication of the Rule in the Federal Register. In addition, depository institutions that previously qualified for the exclusion but subsequently exceed the SBA size standard will be required to comply with the Rule within a reasonable amount of time after exceeding the SBA size standard, such time period not to exceed five (5) years. The Rule defines the "SBA size standard" as the SBA size standard for a data provider's appropriate North American Industry Classification System ("NAICS") code assigned to the entity for commercial banking, credit unions, savings institutions, and other depository credit intermediation, or credit card issuing, under 13 C.F.R. § 121.201. As an example, the SBA size standard for NAICS Code 522110 (commercial banking), covering the activities of accepting demand and other deposits and making commercial, industrial, and consumer loans, is $850 million in assets.

For purposes of the Rule, assets are calculated by averaging the assets reported on a depository institution's four (4) preceding quarterly call reports submitted to the Federal Financial Institutions Examination Council, National Credit Union Association, or other applicable oversight body. The Rule additionally prescribes instructions for the calculation of total assets of depository institutions if four (4) quarterly call reports are not available (for example, in the case of a merger or acquisition).

DATA PROVIDER COMPLIANCE

Compliance with the Rule is expected in stages, based on total asset size for depository institution data providers or total receipts (as defined by the SBA) for nondepository institution data providers.

- Depository institution data providers with total assets of at least $250 billion, and nondepository institution data providers that generated at least $10 billion in total receipts in either 2023 or 2024, are expected to comply with the Rule by **April 1, 2026**.
- Depository institution data providers that hold at least $10 billion in total assets but less than $250 billion in total assets, and nondepository institutions that did not generate at least $10 billion in total receipts in either 2023 or 2024, are expected to comply with the Rule by **April 1, 2027.**
- Depository institution data providers that hold at least $3 billion in total assets but less than $10 billion in total assets are expected to comply with the Rule by **April 1, 2028**.
- Depository institution data providers that hold at least $1.5 billion in total assets but less than $3 billion in total assets are expected to comply with the Rule by **April 1, 2029**.

- Depository institution data providers that hold less than $1.5 billion in total assets but more than $850 million in total assets are expected to comply with the Rule by **April 1, 2030**.

OBLIGATIONS OF AUTHORIZED THIRD PARTIES UNDER THE RULE

Authorization Status: A third party making a request for covered data regarding a product or service the consumer requested must adhere to explicit requirements to provide the consumer with an authorization disclosure, certify that it will agree to the obligations of the Rule, and obtain the consumer's express informed consent to access covered data on behalf of the consumer by obtaining an authorization disclosure that is signed by the consumer electronically or in writing.

Limited Collection, Use, and Retention: The CFPB requires third parties to limit their collection, use, and retention of consumer data to what is reasonably necessary to provide the consumer's requested product or service. Explicitly excluded in the Rule from the phrase "reasonably necessary" is the collection, use, and retention of covered data for purposes of targeted advertising, cross-selling of other products or services, or the sale of covered data. Use of covered data is permitted by the third party (or upon the third party's provision of the data to another third party) for reasons such as:

- to comply with properly authorized legal requests (such as subpoenas or summons), or governmental or regulatory requests;
- to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;
- for purposes of servicing or processing the consumer-requested service or product; or
- for purposes of improving the consumer-requested service or product.

The third party is authorized to collect covered data for a maximum period of one (1) year after the consumer's most recent authorization, after which the third party must follow the procedures in the Rule for subsequent consumer authorization.

Security Requirements: The third party must apply to its systems for the collection, use, and retention of covered data an information security program that satisfies, as applicable, the requirements of Section 501 of the GLBA (and the rules issued pursuant thereto), or the FTC's Standards for Safeguarding Customer Information, 16 C.F.R. Part 314.

Provision of Data to, or Use of, Other Third Parties: Before disclosing covered data to other third parties, the authorized third party must contractually require such other third parties to generally meet the same obligations that it itself is required to meet under Section 1033.421(a) through (e) of the Rule.

To the extent the third party intends to use a data aggregator, the data aggregator is permitted to perform the authorization procedures of the Rule (described in Sections 1033.401) on behalf of the third party seeking authorization to access covered data, so long as the third party seeking authorization remains responsible for compliance with the authorization procedures of Section 1033.401, and the data aggregator makes certain certifications to the consumer about whom the covered data is requested.

Policies and Procedures: The third party must establish and maintain written policies and procedures that are reasonably designed to ensure that (i) covered data is accurately received from a data provider and accurately provided to another third party; (ii) it provides to the consumer, upon request, information keeping the consumer informed about the third party's access to covered data; and (iii) it retains records to evidence its compliance with its requirements under the Rule.

***

Please reach out to any of our FinTech, Banking & Payments attorneys if you have any questions regarding the Rule.
10+ Min Read

Authors

Juan Azel

Carl Fornaris

Jennifer Olivestone

Related Topics

Consumer Financial Protection Bureau (CFPB)

FinTech

Consumer Financial Protection Act (CFPA)

Open Banking

Related Capabilities

Financial Services Transactions & Regulatory

Financial Services Litigation

Financial Services

FinTech, Banking & Payments

Related Professionals

Juan Azel

Carl Fornaris

Jennifer Olivestone