KPMG

Regulatory Alert

Regulatory Insights for Financial Services

October 2024

1033 Open Banking: CFPB Final Rule

KPMG Insights:

- ***Long-time Coming:*** *As part of the Dodd-Frank Act, the finalizing of 'open banking' comes with industry concerns including who shoulders the liability risks, the reputation risks and potential operating costs (including fraud and data breach costs).*
- ***Legal Challenge Initiated:*** *As expected, an industry group lawsuit challenging CFPB authority on 1033 was filed the same day as the final rule release.*
- ***Information/Consumer Protection:*** *Expect expanded regulatory focus on data governance processes and controls (including potential secondary uses of data) to help avert data misuse and breaches.*
- ***Consumer Choice:*** *Update systems and processes to effectively manage/ track consumer preferences (e.g., consent)—while still ensuring the customer experience.*

The Consumer Financial Protection Bureau (CFPB) issues its final rule implementing section 1033 of the Dodd-Frank Act, providing consumers with more choices and direction over their own financial data. Through this rule, the CFPB aims to enhance fair competition, transparency, and accessibility in the markets for consumer financial products and services. The final rule outlines:

- Specific requirements for "data providers" to make "covered data" (including information about transactions, costs, charges, and usage) about "covered financial products and services" available to consumers and to certain "authorized third parties" upon request in a secure and reliable format.
- Obligations for third parties, including data aggregators, accessing consumers' data, including data privacy protections (the CFPB notes that many of these data privacy requirements overlap with the requirements of other State or international data privacy laws).

Applicability. Under the final rule, "data providers" are defined to include 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 (e.g., digital wallet providers).

Note: The rule does not apply to certain small depository institutions as defined by the Small Business Administration (currently set at $850 million or less in total assets). There are no size limitations for non-depository institutions.

Effective and Compliance Date. The final rule goes into effect 60 days after publication in the Federal Register. Compliance with the rule will be phased in over a five-year period based on a calculation of total assets or total receipts (for depository institutions or non-depository institutions, respectively) with the largest entities required to begin compliance by April 1, 2026, and the smallest to begin by April 1, 2030. Data providers must initially comply with the requirements for making covered data available, maintaining data provider interfaces, and responding to requests (Subparts B and C of the final rule).

Requirements

"Data providers" are required to:

- Make available to a consumer and an authorized third party, upon request, covered data in the data providers control or possession concerning a covered consumer financial product or service that the consumer obtained

from the data provider. The data must be made available in an electronic form usable by consumers and authorized third parties. *Note: The CFPB intends on covering more products over time through future rulemaking.*

- Not take any action to evade providing covered data to a consumer or an authorized third party, including actions that the data provider knows or should know is likely to render the data unusable or to materially discourage a consumer or authorized third party from accessing it.
- Make available the most recently updated covered data that it has in its control or possession at the time of a request, including information concerning authorized but not yet settled transactions.
- Maintain a consumer interface that allows consumers to directly access their data as well as a developer interface that meets specific requirements in the rule (e.g., standardized format, minimum performance response rate of 99.5 percent). The data provider may not charge a fee for receiving a request for, or making available, covered data.
- Have policies and procedures covering the accuracy of data transferred to third parties; access denials and denials of information requests; and records retention requirements.

"Authorized Third Parties" acting on behalf of an individual consumer and accessing consumer information are subject to requirements including:

- Providing "authorization disclosures" that:
  - Inform consumers of key terms of access (including general categories of information to be accessed, identity of the covered data provider, accounts to be accessed, terms related to duration and frequency of access, and how to revoke access).
  - Solicit and obtain consumers' consent to the terms of access.
- Issuing consumers with a certification statement on adherence to certain obligations regarding collection, use, and retention of the consumer's information.
- Limiting collection, use, and retention of consumer-authorized information to what is reasonably necessary to provide a product or service and limiting the duration of the covered data collection to a maximum of one year.
- Implementing data security standards to prevent exposing consumers to data security harms (i.e., the requirements of section 501 of the GLBA or FTC's Standards for Safeguarding Customer Information).
- Providing consumers with a simple means to revoke authorization, without cost or penalty.
- Establishing and maintaining systems that receive data access revocation requests, track duration-limited authorizations, and delete data when required due to revoked authorizations, durational periods ending, or because retaining the data is no longer reasonably necessary.
- Retaining records for a period of at least three years.

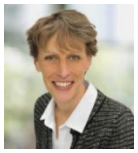
Third parties may provide covered data to other third parties that have agreed, by contract, to comply with the third-party obligations outlined in the rule. Third parties may also use a data aggregator to assist with collecting covered data on behalf of a consumer. The data aggregator must certify that it agrees to the third-party obligations as outlined in the rule.

Definitions

- **Data Provider:** 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.
- **Covered Data:**
  - Transaction information, including historical transaction information, in the control or possession of the data provider.
  - Account balance information.
  - Information to initiate payment to or from a Regulation E account directly or indirectly held by the data provider.
  - Terms and conditions.
  - Upcoming bill information.
  - Basic account verification information (e.g., name, address, email address, phone number).
- **Authorized Third Party:** A third party that has complied with the authorization procedures set forth in subpart D of part 1033.

For more information, contact Amy Matsuo, Nadia Orawski , or Todd Semanco.

Contact the author:



Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com

kpmg.com/socialme