GT GreenbergTraurig

Alert | Financial Regulatory & Compliance

November 2024

CFPB Issues Personal Financial Data Rights Rule

Go-To Guide:

- The CFPB issued a final rule, called the "Personal Financial Data Rights Rule," to implement Section 1033 of Title X of the Dodd-Frank Act.
- The rule will require covered financial institutions to provide consumers and authorized third parties with access and portability options for their financial data.
- The CFPB suggests that the rule will accelerate the shift to open banking and jumpstart competition in banking and consumer finance by making it easier for consumers to switch to new providers.

On Oct. 22, 2024, the CFPB issued a final rule that will require covered financial institutions to provide consumers and authorized third parties with access and portability options for their financial data. The CFPB's final rule, called the "Personal Financial Data Rights Rule," implements Section 1033 of Title X of the Dodd-Frank Act, a to-date dormant provision of law enacted by Congress more than a decade ago.

In a press release announcing the final rule, CFPB Director Rohit Chopra highlighted the CFPB's goal of increasing competition and facilitating a shift to open banking. "Too many Americans are stuck in financial products with lousy rates and service," Chopra said. "Today's action will give people more power to get better rates and service on bank accounts, credit cards, and more."

Background

In Section 1033 of Title X of the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act, Congress directed the CFPB to issue rules requiring covered financial institutions to provide consumers with access and portability options for their financial data,[1] and also directed the CFPB to issue rules prescribing standards to encourage the development and use of standardized data-sharing formats.[2]

Beginning with a 2016 Request for Information, the CFPB has taken several steps to develop rules to implement Section 1033. Among other steps, the CFPB released a related set of consumer protection principles in October 2017; an advanced notice of proposed rulemaking in October 2020; a related report from the Small Business Review Panel in April 2023; and notice of proposed rulemaking in October 2023. In addition, in June 2024, the CFPB issued a final rule outlining the qualifications to become a recognized industry standard setting body, which can issue standards that companies can use to help them comply with the CFPB's Personal Financial Data Rights Rule.

With the issuance of the final Personal Financial Data Rights Rule, the CFPB has taken the final step in its Section 1033 rulemaking process. Since the CFPB issued the rule, two industry group filed lawsuits challenging the CFPB's authority under Section 1033.

The Rule

The CFPB's Personal Financial Data Rights Rule is intended to provide consumers with the right to access their financial data and the right to share that data with others, including other financial services providers. But that is no small task. And, indeed, the CFPB's final rule is relatively complex.

- ***Scope - Data Providers & Third Parties***. The rule creates obligations for "data providers" and "authorized third parties." Subject to an exclusion for "depository institutions that hold assets equal to or less than the SBA size standard" (which, for all relevant NAICS codes, is currently $850 million), a "data provider" includes any "financial institution" as that term is defined in 12 C.F.R. 1005.2(i) (Reg. E); any "card issuer" as that term is defined in 12 C.F.R. 1026.2(a)(7) (Reg. Z); and any "other person that controls or possess information concerning a covered consumer financial product or service the consumer obtained from that person." An "authorized third party" includes any "third party that has complied with the authorization procedures" specified in the final rule.
- ***Scope – Covered Consumer Financial Product or Service***. The rule creates obligations with respect to any "covered consumer financial product or service." A "covered consumer financial product or service" includes any "account" as that term is defined in 12 C.F.R. 1005.2(b) (Reg. E); any "credit card" as that term is defined in 12 C.F.R. 1026.2(a)(15)(i) (Reg. Z); and any product or service that facilitates "payments from a Regulation E account or Regulation Z credit card, excluding products or services that merely facilitate first party payments."
- ***Scope – Covered Data***. The rule creates obligations with respect to "covered data." Subject to certain specified exceptions, "covered data" includes transaction information—including the amount, transaction data, payment type, pending or authorized status, payee or merchant name, rewards

[1] 12 U.S.C. § 5533(a) ("Subject to rules prescribed by the Bureau, a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data. The information shall be made available in an electronic form usable by consumers.").
[2] 12 U.S.C. § 5533(d) ("The Bureau, by rule, shall prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine-readable files, to be made available to consumers under this section.").

credits, and fees or finance charges—and account balance information, payment initiation data (e.g., account and routing number), terms and conditions, upcoming bill information, and basic account verification information.

- ***Data Provider Obligation – Data Access***. Subject to certain exceptions, a data provider is required to provide an authenticated consumer or an authorized third party any covered data in the data provider's control or possession concerning a covered consumer financial product or service that the consumer obtained from the data provider. The covered data must be provided in an "electronic form usable by consumers and authorized third parties." And the data provider is not permitted to impose any fee or charge on the consumer or authorized third party in connection with any data access request.
- ***Data Provider Obligation – Consumer Interface & Developer Interface & Data Security***. A data provider is required to maintain a "consumer interface" and a "developer interface" through which it receives and responds to requests for covered data from consumers and authorized third parties, respectively, and to protect the developer interface with an information security program that satisfies the applicable rules issued pursuant to section 501 of the Gramm-Leach-Bliley Act (GLBA) or, if a data provider is not subject to the GLBA, the FTC's Safeguards Rule.
- ***Data Provider Obligation – Written Policies and Procedures***. A data provider is required to "establish and maintain written policies and procedures that are reasonably designed to achieve the objectives" of the rule and to "ensure retention of records that are evidence of compliance."
- ***Authorized Third-Party Obligation – Processing Limitations***. An authorized third party's collection, use, and retention of any covered data must be limited to what is "reasonably necessary to provide the consumer's requested product or service," which includes uses "that are specifically required under other provisions of law," "that are reasonably necessary to . . . prevent actual or potential fraud, unauthorized transactions, claims, or other liability," and "that are reasonably necessary to improve the product or service the consumer requested." Targeted advertising, cross-selling of other products or services, and the sale of covered data are not "part of, or reasonably necessary to, any product or service." And the authorized third party is required to "limit the duration of collection of covered data to a maximum period of one year after the consumer's most recent authorization."
- ***Authorized Third-Party Obligation – Data Security***. An authorized third party must protect the systems it uses for the collection, use, and retention of covered data with an information security program that satisfies the applicable rules issued pursuant to section 501 of the GLBA.
- ***Authorized Third-Party Obligation – Written Policies and Procedures***. An authorized third party is required to "establish and maintain written policies and procedures that are reasonably designed to ensure that covered data are accurately received from a data provider and accurately provided to another third party," to ensure that it provides consumers with the required information, and to "ensure retention of records that are evidence of compliance."
- ***Phased Implementation***. Larger data providers will be subject to the proposed rule's requirements sooner than smaller institutions, with the compliance deadline for the largest depository institutions subject to the rule on April 1, 2026, and that for the smallest depository institutions are subject to the rule, on April 1, 2030.

Takeaways

The CFPB's final rule implementing Section 1033 will accelerate a shift to open banking and increase competition among certain types of financial services providers. But it will also create a new and potentially burdensome regulatory regime. Covered entities should closely examine the final rule, consider whether it creates business opportunities or risks, and consider whether current technology and operations-directed investments will facilitate compliance with the rule.

Authors

This GT Alert was prepared by:

- Timothy A. Butler | +1 678.553.2326 | Tim.Butler@gtlaw.com
- Matthew M. White | +1 678.553.2111 | Matthew.White@gtlaw.com
- Tessa L. Cierny | +1 678.553.2130 | Tessa.Cierny@gtlaw.com