

Alert | Financial Regulatory & Compliance



October 2023

CFPB Issues Proposed ‘Personal Financial Data Rights’ Rule

Go-To Guide:

- The Consumer Financial Protection Bureau (CFPB) has issued a proposed rule, called the “Personal Financial Data Rights” rule, to implement Section 1033 of Title X of the Dodd-Frank Act.
- If finalized in its present form, the proposed rule would 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 proposed 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.
- Comments on the CFPB’s proposed rule are due on or before Dec. 29, 2023.
- The CFPB is expected to issue its final rule implementing Section 1033 in the fall of 2024.

On Oct. 19, 2023, the CFPB released a **proposed rule** that, if finalized in its present form, would require covered financial institutions to provide consumers and authorized third parties with access and portability options for their financial data. The CFPB’s proposed rule, called the “Personal Financial Data Rights” rule, would implement 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 proposed rule](#), CFPB Director Rohit Chopra highlighted the CFPB’s goal of increasing competition and facilitating a shift to open banking. “With the right consumer protections in place, a shift toward open and decentralized banking can supercharge competition, improve financial products and services, and discourage junk fees,” Chopra said. “Today, we are proposing a rule to give consumers the power to walk away from bad service and choose the financial institutions that offer the best products and prices.”

In separate [prepared remarks](#), Director Chopra said the CFPB “will look to finalize the rule by next fall.” He also stressed the importance of the proposed rule. “Over time, I hope our work to activate this dormant authority, jumpstart competition, and promote decentralization in finance will help American families put billions of dollars in their pockets, while allowing small players startups to go head-to-head with major market players,” he said.

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; and a related [report from the Small Business Review Panel in April 2023](#).

With the release of its proposed rule, the CFPB has taken one of the final steps in its Section 1033 rulemaking process. The CFPB will now collect comments on the proposed rule through Dec. 29, 2023, and then probably issue a final rule implementing Section 1033 in the fall of 2024, as Director Chopra noted in his prepared remarks.

The Proposed Rule

The CFPB’s proposed Personal Financial Data Rights Rule intends 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 proposed rule is relatively complex.

- *Scope - Data Providers & Third Parties.* The proposed rule would create obligations for “data providers” and “authorized third parties.” Subject to an exclusion for “depository institutions that do not have a consumer interface,” a “data provider” would include 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 possesses information concerning a covered consumer financial product or service the consumer obtained from that person.” An

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.”).

“authorized third party” would include any “third party that has complied with the authorization procedures” specified in the proposed rule.

- *Scope – Covered Financial Product or Service.* The proposed rule would create obligations with respect to any “covered financial product or service.” A “covered financial product or service” would include 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.”
- *Scope – Covered Data.* The proposed rule would create obligations with respect to “covered data.” Subject to certain specified exceptions, “covered data” would include transaction information, account balance, payment-initiation information to or from a Regulation E account, terms and conditions, upcoming bill information, and basic account verification information.
- *Data Provider Obligation – Data Access.* Subject to certain exceptions, a data provider would be required to provide an authenticated consumer, an authorized third party, or a data aggregator acting for an authorized third party with the most recently updated covered data in the data provider’s control or possession concerning any covered consumer financial product or service that the consumer obtained from the data provider. The covered data would have to be provided in an “electronic form usable by consumers and authorized third parties.” And the data provider would not be permitted to impose any fee or charge on the consumer or authorized third party in connection with any data access request.
- *Data Provider Obligation – Developer Interface & Data Security.* A data provider would be required to create a “developer interface” through which it receives and responds to requests for covered data, and to protect that developer interface with an information security program that satisfies the applicable rules issued pursuant to the Gramm-Leach-Bliley Act.
- *Data Provider Obligation – Written Policies and Procedures.* A data provider would be required to “establish and maintain written policies and procedures that are reasonably designed to achieve the objections” of the proposed 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 would be limited to what is “reasonably necessary to provide the consumer’s requested product or service.” Targeted advertising, cross-selling of other products or services, and the sale of covered data would not be “part of, or reasonably necessary to, any product or service.” And the authorized third party would be 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 the Gramm-Leach-Bliley Act.
- *Authorized Third Party Obligation – Written Policies and Procedures.* An authorized third party would be 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 providers³ would be subject to the proposed rule's requirements sooner than smaller institutions, while community banks and credit unions without a digital interface would be exempt.

Takeaways

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

Stakeholders should submit comments on any aspect of the proposed rule by Dec. 29, 2023.

Authors

This GT Alert was prepared by:

- **Timothy A. Butler** | +1 678.553.2326 | Tim.Butler@gtlaw.com
- **Benjamin M. Saul** | +1 202.331.3123 | saulbe@gtlaw.com
- **Tarrian L. Ellis** | +1 202.533.2351 | Tarrian.Ellis@gtlaw.com
- **Matthew M. White** | +1 678.553.2111 | Matthew.White@gtlaw.com
- **Tessa L. Cierny** | +1 678.553.2130 | Tessa.Cierny@gtlaw.com
- **Zeba Pirani** ~ | Law Clerk/JD | Atlanta

~ *Not admitted to the practice of law.*

Albany. Amsterdam. Atlanta. Austin. Berlin.→ Boston. Charlotte. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Houston. Kingdom of Saudi Arabia.« Las Vegas. London.* Long Island. Los Angeles. Mexico City.+ Miami. Milan.» Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Portland. Sacramento. Salt Lake City. San Diego. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Singapore.° Tallahassee. Tampa. Tel Aviv.^ Tokyo.⋈ United Arab Emirates.< Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. →Greenberg Traurig's Berlin office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. «Khalid Al-Thebity Law Firm in affiliation with Greenberg Traurig, P.A. is applying to register a joint venture in Saudi Arabia. *Operates as a separate UK registered legal entity. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's Milan office is operated by Greenberg Traurig Santa Maria, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. °Greenberg Traurig's Singapore office is operated by Greenberg Traurig Singapore LLP which is licensed as a foreign law practice in Singapore. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. ⋈Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojimbengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. <Greenberg Traurig's United Arab Emirates office is operated by Greenberg Traurig Limited. ~Greenberg Traurig's Warsaw office is operated by GREENBERG*

³ Depository institution data providers that hold at least \$500 billion in total assets and non-depository institution data providers that generated at least \$10 billion in revenue in the preceding calendar year or are projected to generate at least \$10 billion in revenue in the current calendar year.

TRAURIG Nowakowska-Zimoch Wysokiński sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in GREENBERG TRAURIG Nowakowska-Zimoch Wysokiński sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2023 Greenberg Traurig, LLP. All rights reserved.