Cooley

CFPB Proposes Financial Data and Open Banking Rule

October 27, 2023

On October 19, 2023, the Consumer Financial Protection Bureau (CFPB) issued a notice of proposed rulemaking to implement Section 1033 of the Dodd-Frank Act. Section 1033 of Dodd-Frank requires covered persons to make information concerning a financial product or service that a consumer has obtained from such person available to the consumer, subject to rules implemented by the bureau.

The proposed rule would require that certain financial institutions, card issuers and other payment facilitation providers make consumer data – including transaction data – more readily available to consumers and authorized third parties. It also would place consumer protection obligations on these entities, as well as on third parties authorized to collect and use that data.

Who would be required to provide data under the rule?

The proposed rule would apply to "data providers" – generally, financial institutions that offer consumer deposit accounts subject to the Electronic Funds Transfer Act (EFTA), credit card issuers subject to the Truth in Lending Act (TILA) and entities that offer related payment facilitation products and services. As a result, most banks would be covered, as would digital wallet providers and neobanks. Entities without consumer-facing digital banking interfaces, as of the rule's compliance date, would be excluded from coverage.

What data would be covered by the rule?

Under the proposal, data providers would be responsible for providing consumer and authorized third-party access to "covered data," which would include 24 months of transaction data, certain account information (e.g., account balance, upcoming bills, basic account verification), information to initiate payment to and from accounts, and the terms and conditions under which the account or card was provided (e.g., APR, reward program terms, etc.).

Confidential commercial information, information collected solely to prevent fraud, money laundering, and other unlawful conduct, information required by law to be kept confidential, and information that cannot be retrieved in the ordinary course of business would not be subject to the rule's requirements.

How would data providers be obligated to make covered data available?

The proposal would require that data providers maintain consumer interfaces and establish and maintain developer interfaces to allow consumer and third-party access to data.

The proposed rule would prohibit data providers from imposing any fees or charges on consumers or authorized third parties for establishing and maintaining – or making data available through – the interfaces. It also would require providers to publicly disclose (e.g., on a website) developer interface and contact information to facilitate access and provide a method to address questions.

Importantly, with respect to their developer interfaces, the proposed rule also would require that data providers:

- Not rely on screen scraping – a technology that leverages consumer credentials to log into accounts to retrieve data, meaning such interfaces would likely take the form of application program interfaces (APIs).
- Make covered data available in a standardized format based on "qualified industry standards," or in a format "widely used by the developer interfaces of other similarly situated data providers with respect to similar data and [that] is readily usable by authorized third parties."
- Make data available, through such interfaces, after obtaining information sufficient to authenticate the third party and consumer, confirming that the third party has obtained consumer authorization and verifying the scope of the data request.
- Not unreasonably restrict the frequency with which they accept and respond to data requests.
- Ensure their developer interfaces perform at a "commercially reasonable" level – including that such interfaces have a data access request response rate, calculated consistent with the rule, of at least 99.5%.
- Apply an information security program to the interface that complies with the Gramm-Leach-Bliley Act (GLBA) or, if not subject to the GLBA, the information security program requirements of the Federal Trade Commission's (FTC) Safeguards Rule.

What obligations would be imposed on third parties authorized to access and collect consumers' data?

The proposed rule would require authorized third parties to implement safeguards around the collection, use and retention of such data. In order to access consumers' covered data, the proposed rule would, for example, require authorized third parties to:

- Provide the consumer with a comprehensive authorization disclosure.
- Certify to the consumer – within the authorization disclosure – that the third party agrees to limit the collection, use and retention of covered data, and apply to that collection, use and retention a GLBA-compliant information security program or, if not subject to the GLBA, the information security requirements of the FTC Safeguards Rule.
- Obtain the consumer's "express informed consent" to key terms of access through a signed authorization disclosure, either electronically or in writing.
- Provide the consumer with a signed copy or otherwise agreed to copy of the authorization disclosure and the third party's contact information in case of any questions.

As reflected by the certification requirement identified above, the proposed rule would only permit third parties to collect, use and retain data as "reasonably necessary" to provide the consumer with the requested product or service. Third parties would therefore be prohibited from using data for most other purposes, including for targeted advertising, cross-selling products or services, or sale to data brokers.

Additional limitations on authorized third parties include a requirement to obtain reauthorization from consumers to continue to collect data after one year. Third parties that fail to obtain reauthorization would be required to delete previously collected data unless that data is reasonably necessary to provide the product or service requested by the consumer.

What role do data aggregators play – and what obligations do they have – with respect to the collection of covered data?

The proposed rule also would allow third parties to use "data aggregators" to access covered data, subject to disclosure and certification requirements. The authorization disclosure presented by a third party to the consumer would need to identify any aggregators used by the third party.

Like authorized third parties, data aggregators also would need to certify to the consumer – either as part of the authorized third

party's disclosure or separately – that they agree to comply with the rule's data access conditions and restrictions. The authorized third party, however, would ultimately be responsible for compliance with the proposed rule's authorization procedures.

Looking ahead

CFPB Director Rohit Chopra stated that the proposed rule is meant to "accelerate much-needed competition and decentralization in banking and consumer finance" while at the same time providing "strong data protections to prevent misuse and abuse of personal financial data." This commentary, and the rule itself, align with the continued CFPB refrain to industry about the consumer benefits of increasing competition within the banking markets while ensuring robust controls in protecting consumer data. This includes commitments from the CFPB to pursue insufficient data protection or security as a violation of the Consumer Financial Protection Act's prohibition on unfair, deceptive or abusive acts and practices. Indeed, the press release accompanying the proposed rule adopts the same aggressive tone the industry has come to expect from the CFPB, with references to eliminating "data hoarding" and empowering consumers to access information absent junk fees.

The rule also establishes clear record requirements designed to facilitate supervision and enforcement of compliance with the rule not just by the CFPB, but also by "Federal and State banking regulators, State attorneys general, and other government agencies that supervise data providers."

Entities that come within the scope of the proposed rule should take note and begin to evaluate how it might impact their processes. For example, entities that the rule would treat as authorized third parties may want to consider the potential implications of needing to align their information security practices to the FTC's Safeguards Rule if not subject to the GLBA.

Those entities currently outside the scope of the proposed rule should also pay attention. As highlighted in the press release, this is just the first proposal to implement Section 1033. The "CFPB intends to cover additional products and services in future rulemaking." To that end, the CFPB is seeking comment on whether electronic benefit transfer (EBT) cards, otherwise exempt from EFTA coverage, should be included in the scope of the proposed rule and also whether historical information should be made available for more categories of covered data.

In terms of next steps, comments on the proposed rule are due on or before December 29, 2023. The bureau stated that it will seek to finalize the rule by fall 2024.

Please join us for a webinar to discuss the latest updates concerning the CFPB's proposed open banking rule. Register here.

Key Contacts

Jessica Pollet Santa Monica	jpollet@cooley.com +1 310 883 6529
Michelle L. Rogers Washington, DC	mrogers@cooley.com +1 202 776 2227