STINSON

News & Insights

CFPB Promotes Open Banking as it Issues Final Rule on Personal Financial Data Access Rights

Alert
10.28.2024

By Heidi Wicker, Anastasia Stull, Michelle Fox, Tom Witherspoon & Matthew Grimaldi

Time will tell whether the Consumer Financial Protection Bureau's (CFPB) stated goals of accelerating "open banking" and competition will come to fruition as a result of the long-awaited final rule implementing Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.

What is evident, however, is that there will be immediate business/financial, technological and operational impacts across the U.S. banking and payments ecosystem – affecting depository institutions, card issuers, digital wallet providers and other FinTechs alike – all of whom may have compliance obligations under the rule.

The rule imposes obligations on two groups of players: data providers and requestors, which may be either consumers themselves or third parties authorized by the consumer. It is quite possible that an entity may be both a data provider and an authorized third-party requestor, depending upon its business model. We summarize both categories of obligations below.

OBLIGATIONS ON DATA PROVIDERS

The rule requires "data providers" to, upon request, make available covered data about covered financial products and services in electronic form to a) the consumer to whom it pertains or b) a third-party the consumer authorizes. No fee may be charged by the data provider to a consumer or authorized third party for requesting covered data.

The first step of determining whether a data provider is within the scope of the rule is to determine whether one controls or possesses "covered data" concerning a "covered consumer financial product or service" that the consumer obtained from the data provider.

CFPB Promotes Open Banking as it Issues Final Rule on Personal Financial Data Access Rights

A "covered consumer financial product or service" is defined as:

- An account, as defined under federal Regulation E;
- A credit card, as defined under federal Regulation Z; or
- Facilitation of payments from a Regulation E account or Regulation Z credit card, excluding first party payments initiated by the payee or its agent.

"Covered data" means, as applicable:

- Transaction information;
- 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; and
- Basic account verification information.

The rule goes on to state that one must be a "covered person" under 12 U.S.C. § 5481(6) that is:

- A financial institution as defined under Regulation E;
- A card issuer as defined under Regulation Z; or
- Any other person that controls or possesses information concerning a covered consumer financial product or service that the consumer obtained from that person (e.g., a digital wallet provider).

A data provider must make certain information about itself readily available, including contact information for consumers or third parties with questions about accessing covered data. Data must be provided in response to requests in an electronic form usable by consumers and authorized third parties, and must include the most recently uploaded covered data that the data provider has in its control or possession at the time of a request (including authorized, but not yet settled, transactions).

The rule includes a prohibition against evasion of the rule; however, there are several permitted exceptions to a data provider's obligation to provide information to a consumer or authorized third party, namely:

- Certain confidential commercial information;
- Information required to be kept confidential by law (such as suspicious activity reports);
- Information collected by the data provider for the sole purpose of preventing fraud or money laundering, or detecting or reporting unlawful conduct; and

- Any information the data provider cannot retrieve in the ordinary course of its business.

Further, if the data provider is a depository institution that does not hold total assets equal to or less than the Small Business Administration's size standard for its North American Industry Classification System code (currently $850 million for all relevant codes) by averaging their assets on the four preceding call reports, the rule does not apply. Institutions do not fall out of coverage under the rule simply because their assets dip below the threshold; rather, once an institution has become capable of complying, it must continue to comply.

For security purposes, data providers may request certain verification information prior to making covered data available to a consumer or a consumer's authorized third party.

THIRD-PARTY AUTHORIZATION AND ACCESS

Importantly, a third party may only collect, use or retain information received from the data provider that is reasonably necessary to provide a product or service requested by the consumer. The rule expressly states that targeted advertising, cross-selling or the sale of covered data are not "reasonably necessary" to provide any other product or service.

To become authorized, a third party must seek access from a data provider on behalf of a consumer to provide a product or service the consumer requested, and must:

- Provide the consumer with an authorization disclosure meeting specified content and delivery requirements;
- Certify in the authorization disclosure that the third party agrees to its obligations under the rule; and
- Obtain the consumer's express informed consent to access covered data via an authorization disclosure signed by the consumer electronically or in writing.

CONSUMER AND DEVELOPER INTERFACES AND DATA SECURITY

Data providers covered under the final rule must maintain both a consumer interface and a developer interface and make covered data available via both in a standardized and machine-readable format. The CFPB previously issued another rule (Required Rulemaking on Personal Financial Data Rights; Industry Standard-Setting), outlining how entities may apply for recognition as a standard-setting body. Entities who become recognized will help shape the standards for the format of data transmitted.

Data providers subject to section 501 of the federal Gramm-Leach-Bliley Act (GLBA) must apply an information security program to the developer interface that satisfies the applicable rules issued pursuant to section 501 of the GLBA. Otherwise, data providers must apply the information security program

required by the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 C.F.R. part 314. Moreover, data providers must not allow any third party to access the data provider's developer interface by using any credentials that a consumer uses to access the consumer interface (i.e., no screen scraping).

COMPLIANCE/IMPLEMENTATION DATES

The final rule becomes effective 60 days after publication in the *Federal Register*. Compliance deadlines begin April 1, 2026, for depository institution data providers holding at least $250 billion in total assets and nondepository institution data providers who generated at least $10 billion in total receipts in either calendar year 2023 or calendar year 2024.

Smaller data providers have compliance deadlines on April 1 of the following four years after the initial deadline (through 2030).

FINAL THOUGHTS

On the same day the final 1033 rule was published, the Banking Policy Institute, Forcht Bank, N.A., and Kentucky Bankers Association sued the CFPB in the U.S. District Court for the Eastern District of Kentucky. Plaintiffs are seeking declaratory and injunctive relief and challenging the CFPB's statutory authority. We recommend preparing for compliance with the rule, as it is too soon to know whether this court will stay the implementation of the rule.

The CFPB has made it clear that this is just the first rule it is issuing intended to accelerate responsible "open banking," and it will be developing others to address more products, services and use cases.

CONTACTS

Michelle A. Fox

Matthew Grimaldi

Anastasia D. Stull

Heidi S. Wicker

Thomas C. Witherspoon

RELATED CAPABILITIES

Banking & Financial Services

FinTech, Payments & Financial Products