Articles + Publications | March 14, 2024

Banks Should Continue to Prep for CFPB Data Rule Rollout

WRITTEN BY

Keith J. Barnett | Carlin A. McCrory | Benjamin W. White | Joshua McBeain

Published in Law360 on March 14, 2024.

Companies that fall within the definition of "data provider" are expected by this fall to be required to comply with the Consumer Financial Protection Bureau's **proposed rule** implementing Section 1033 of the Dodd-Frank Act.

In a press release issued Oct. 19, 2023, the CFPB touted the proposed rule as one that "would accelerate a shift toward open banking, where consumers would have control over data about their financial lives and would gain new protections against companies misusing their data."

In a nutshell, if the proposed rule becomes final as drafted, certain depository and nondepository entities, defined as data providers, will be required to make specific account data available to consumers and authorized third parties. These data providers will also be required to establish obligations for the third parties seeking access to the consumer data.

Entities currently supervised by the CFPB, such as banks and credit unions with more than $10 billion in assets, should expect compliance with the proposed rule to be a part of their CFPB supervisory examinations. Entities with less than $10 billion in assets that are supervised by the Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation or National Credit Union Administration should likewise expect compliance with the proposed rule to be a part of their supervisory examinations. State regulators and state attorneys general will also be able to enforce the rule against covered entities.

Before the comment period closed on Dec. 29, 2023, the CFPB received more than 11,000 comments from financial institutions, consumer protection groups, neo-banks, fintechs and other voices in the industry.

Affected financial institutions should be getting ready for the rule, if they have not already done so, by analyzing the proposed rule, determining whether they or their vendors must comply, and making sure they will have the technological and human resources that will allow them to fully comply with their respective compliance deadlines.

Requirements for Data Providers

Data providers must make personal financial data available, at no charge to consumers, through dedicated secure digital interfaces.

Data providers are financial institutions as defined in Regulation E, card issuers as defined in Regulation Z, and "any other person that controls or possesses information concerning a consumer financial product or service the consumer obtained from that person."

In addition to financial institutions, entities that fall within this definition can include nondepository institutions such as mortgage servicers, debt collectors and prepaid card providers.

Depository institutions that do not offer mobile or online banking will be exempt from the rule.

Consumers will have the right to authorize third parties to access information associated with their credit cards and checking, prepaid and digital wallet accounts, and to revoke said access.

Data providers will be required to establish interfaces to make data available in a standardized machine-readable format. The CFPB's goal is to end the "screen-scraping" method of data access, where consumers provide their usernames and passwords to third parties, so the third parties can access consumer data possessed by data providers.

Data providers must "establish and maintain written policies and procedures" to implement the CFPB's objectives and "ensure retention of records that are evidence of compliance."

How Data Providers and Third Parties Should Prepare

The CFPB has proposed a tiered compliance rollout, requiring the largest depository institution data providers to comply in the first six months of the effective date. That compliance will gradually expand to smaller providers over the next four years.

Given this timeline, data providers should start working on their compliance framework as follows.

Interfaces for Consumers and Developers

Certain data providers will be required to provide covered data about covered financial products or services. Covered data includes transaction information, account balance, payment initiation to or from a Regulation E account, terms and conditions, upcoming bill information, and basic account verification information.

Covered data does not include confidential commercial information, which includes algorithms "used to derive credit scores or other risk scores or predictors;" information collected for the sole purpose of preventing fraud or unlawful conduct; information required by law to remain confidential; and information that the data provider cannot retrieve in the ordinary course of business.

Data providers must prepare digital consumer and developer interfaces that will allow consumers and authorized third parties to request and access covered data. A developer interface is a portal through which a data provider receives requests for, and makes available, covered data in an electronic form usable by authorized third parties.

The CFPB envisions multiple additional criteria for developer interfaces and intends to use the developer interface

requirements to move the industry away from screen-scraping of unstructured data. A developer interface will require covered data to be provided in a standardized format, with certain performance and security standards.

Covered financial institutions should accordingly begin to develop software applications to provide consumer and developer interfaces by reviewing third-party vendor solutions or building their own platforms.

Compliant Data Access and Denial of Access

Data providers will generally be required to make data available to consumers wherever they provide information sufficient to authenticate their identity and identify the scope of the data requested.

Similarly, data providers must make data available when a third party provides information sufficient to allow the data provider to authenticate the consumer's identity, authenticate the third party's identity, confirm the third party has followed the authorization procedures and identify the scope of the data request.

Data providers can withhold data from a person or entity that presents significant risks to the data provider's security or risk management program, provided that the denial is reasonable.

Data providers can also withhold data from a third party that does not present evidence that its data security practices are adequate to safeguard the covered data, or when the third party withholds certain information about itself. The data provider can also deny access to a third party if a third party's authorization is no longer valid.

Clear compliance programs must be in place, along with adequately trained personnel, because any denial must be applied in a consistent and nondiscriminatory manner.

Public Disclosure Requirements

Data providers will also be required to publish on their website, in a readily identifiable manner, certain information about themselves. This information includes identifying information, contact information, and information about their developer interfaces in human and machine-readable formats.

In a readily identifiable manner, data providers must publicly disclose documentation, including metadata, that describes all covered data and its corresponding data fields, along with other documentation sufficient for a third party to access and use the developer interface.

Data providers must also publish on their respective websites, on or before the 10th calendar day of each month, the percent of requests for covered data received by its developer interface in the preceding calendar month for which the interface provided a response.

Record Retention and Written Policies and Procedures

Data providers and authorized third parties must develop written policies and procedures to ensure retention of records that show compliance.

These policies and procedures for data providers must address covered data availability, including what is not made available through exceptions and data request denials; covered data accuracy, including specific enumerated elements that must be considered when designing the policies and procedures; and record retention, which lasts three years for third-party requests for information and what the proposed rule calls a "reasonable period of time" for all other records.

The policies and procedures must be appropriate to the size, nature and complexity of the data provider's activities. The required policies and procedures must be periodically reviewed and updated.

Not only must covered entities draft and implement appropriate policies and procedures, relevant personnel must be aware of and trained on said policies and procedures. Personnel should have a clear line of report who can answer any questions that may arise to ensure compliance.

Compliance Dates

The following table illustrates the approximate compliance timeline for each category of data provider.

Tier	Timeline	Criteria
1	6 Months	Depository institution data providers that hold at least $500 billion in total assets, and nondepository 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.
2	1 Year	Depository institutions that hold at least $50 billion in total assets but less than $500 billion in total assets, and nondepository institutions that generated less than $10 billion in revenue in the preceding calendar year, and are projected to generate less than $10 billion in revenue in the current calendar year.
3	2.5 Years	Depository institutions that hold at least $850 million in total assets but less than $50 billion in total assets.
4	4 Years	Depository institutions that hold less than $850 million in total assets.

Industry Reaction to the Proposed Rule

While CFPB Director Rohit Chopra praised the proposed rule as a substantial step toward "open and decentralized banking [that] can supercharge competition, improve financial products and services, and discourage junk fees," some of the comments submitted to the CFPB **from the financial services industry** do not paint such a rosy picture.

Financial institutions and other data providers expressed concerns about the implementation timeline. Data providers also raised concerns about the substantial investment necessary to build and maintain the required interfaces that will facilitate the sharing of the information, and the inability to charge a reasonable fee for access to the information.

Many commenters also raised the issue that the proposed rule's technical specifications are defined with

reference to “qualified industry standards” that are yet to be determined.

Due to the current ambiguities in the proposed rule and the short implementation timelines, many commenters requested that the compliance time frames be extended to allow them time to build compliant systems.

The CFPB also received a significant number of comments from individual consumers. Many of the consumer comments asked the CFPB to include electronic benefit transfer accounts in the final rule.

The comments submitted to the CFPB by the financial services industry reflect those made publicly by banking organizations. The Independent Community Bankers of America stated in a Dec. 29 comment letter to the CFPB that the proposed rule will impose “significant technological burdens and financial costs on community banks.” To offset these costs without passing them to the consumer, the community bankers association suggested banks should be allowed to charge third parties a reasonable fee for access to consumer information.

In its own Dec. 29 comment letter, the American Bankers Association echoed the Independent Community Bankers of America’s call to permit recoupment of costs through fees. The association also pointed out that the proposed rule may create additional issues the CFPB will need to resolve.

For example, the banking association would like the CFPB to take a more active role in managing the proposed data-sharing system, provide banks more flexibility to manage risk and prevent fraud, clarify that data providers under Section 1033 are not furnishers under the Fair Credit Reporting Act and generally tailor the rule to avoid confusion.

The association also stated the proposed rule should be limited to facilitating access to consumer information, without going so far as to mandate conducting payments.

Banking organizations were not the only critics. Rep. Patrick McHenry, R-N.C., the top Republican on the House Financial Services Committee, warned in a Dec. 18 comment letter that

> completely prohibiting the use of secondary data … would prevent financial institutions and third-party service providers from improving on existing products or services (including the very product or service the customer has requested); or building new products or services (including products and services that may be substantially similar to the product or service the consumer has requested).

Conclusion

The CFPB does not typically make changes to proposed rules after receiving comments. Therefore, data providers, third parties and others affected by the proposed rule should begin to adjust their compliance framework and operations accordingly.

RELATED INDUSTRIES + PRACTICES

- Consumer Financial Services