What To Know About CFPB's Financial Data Rights Proposal

By **Denise Barnes, Brandy Bruyere and Molly McGinley** (December 12, 2022)

Denise Barnes

Brandy Bruyere

Molly McGinley

In October, the Consumer Financial Protection Bureau took a significant step forward in enhancing consumer control over private financial data when it launched a rulemaking process under Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act.

Section 1033 requires the CFPB to implement a rule to allow consumers to access their financial information. Currently, there is no duty under Section 1033 to maintain or keep any information about a consumer.

The CFPB has yet to adopt a rule relating to data access, despite its authority to do so.

A data rights rule would not only require financial institutions to share information with consumers, but also empower consumers to more easily switch banks due to poor service.

Banks and other financial institutions would lose one of the primary reasons that banks cross-sell to customers: customer stickiness.

In fact, one of the CFPB's goals in rulemaking[1] is to "create a marketplace where companies would need to improve their offerings to keep their customers." In short, this rule should arguably drive innovation and competition among banks resulting in better products for customers.

Proposals being considered include how and when covered data providers would need to make consumer information available, authorized third party collection, use and retention of consumer information, and record retention obligations and the implementation period for a final rule.

Here are some high-level details from the CFPB's proposals.

Scope and Applicability of Coverage

The CFPB is considering various proposals to implement Section 1033, including which entities would be required to comply and what information a rule would apply to.

Covered data providers in the outline[2] include financial institutions and card issuers. In this context, a financial institution means

> a bank, savings association, credit union, or any other person that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide electronic fund transfer services.

Likewise, here, card issuer means "a person that issues a credit card or that person's agent with respect to the card." Covered accounts in this outline include asset accounts and credit card accounts. These terms align with existing regulatory definitions.

There are six categories of information that the proposals consider making available in connection with covered accounts:

- Periodic statement information for settled transactions and deposits;
- Information regarding prior transactions and deposits that have not yet settled;
- Other information about prior transactions not typically shown on periodic statements or portals;
- Online banking transactions that the consumer has set up, but that have not yet occurred;
- Account identity information; and
- Other information such as agency consumer reports, covered data provider fees, bonuses and rewards, and security breaches.

Third-Party Relationships

Third parties with authorization to access consumer financial information would also have obligations under the proposal rule.

The CFPB has requested feedback on whether the data recipient and the data aggregator should be responsible for the obligation to protect consumer information accessed by third parties.

The CFPB proposals consider collection, use and retention of consumer financial information, and pose several questions in seeking public feedback.

For example, when a consumer gives authorization to a third party to access its information, when and how does a consumer revoke that access?

What if a consumer wants to put limitations on the authorization of third parties who are accessing their financial information? Does a consumer have a responsibility to contact the third party regarding deletion of information?

The CFPB proposals also contemplate consumers' ability to allow third-party access to information and limitations involving access only to information needed to provide a particular product or service. The proposals also look at duration and frequency limits.

The CFPB also is considering accuracy standards relative to third parties' use of consumer data. Third parties could be required to implement and maintain policies and procedures that would verify the accuracy of information and handle consumer disputes.

Compliance Considerations

While the process is in the early stages, the CFPB is not known for giving the industry ample time to comply with new requirements, so institutions affected by the proposed rule should consider the following points, among others, when preparing for future implementation.

First, institutions should consider identifying sources of the relevant financial data early that will aid future compliance efforts.

Again, the proposed rule implicates a broad swath of data, so financial institutions and card issuers can start mapping where such data is housed and what historical data is available.

Moreover, having a clear understanding of the proposed rule and the sources of potential data can help institutions to get ahead of the likely pain points, have a preliminary plan for tackling operational headwinds, and ensure successful implementation.

Second, compliance will likely implicate multiple third parties as well. As consumers would be empowered to authorize third parties to access data, institutions may be required to establish portals to facilitate this process.

If third-party vendors are used to house or facilitate the transfer of the proposed data, institutions should consider how to ensure the accuracy of the data conveyed on their end and exercise appropriate oversight to ensure that the integrity of the data is being maintained.

Third, institutions holding such data will need to track and retain records showing that consumers properly provided such consent to a third party seeking data.

Additionally, vendors will be key partners in tracking much of the financial data that will be covered under the future final rule or building any required data portal.

These relationships will be important when the time is ripe to implement the data rights rule, and vendor management processes will help ensure an institution's partners are well positioned to provide any necessary support to come into compliance on time.

Finally, institutions should consider what additional safeguards, if any, are needed to protect against illegal actions by third parties seeking to compromise or simply access the financial data for pecuniary gain.

This could include hackers as well as other legitimate applications that would seek the information for marketing and other purposes. Institutions will need to reevaluate and potentially strengthen existing cybersecurity safeguards to protect against these threats.

Enforcement Considerations

Although the hope is that with a sufficient investment in compliance and controls, enforcement actions will be curtailed, we don't live in a perfect world.

Financial institutions should anticipate that this rule will undoubtedly lead to some enforcement action by the relevant regulatory agencies, even the U.S. Department of Justice.

Section 1300 does not have an express private right of action, which means that enforcement of any potential rule would be handled by the CFPB, the relevant prudential regulator — i.e., the Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation and the National Credit Union Administration — state financial regulatory agencies and state attorneys general, all of which may impose monetary penalties.

The CFPB proposal also is silent on whether a violation of any future rule would constitute an unfair, deceptive or abusive act or practice, or UDAAP, in violation of the Dodd-Frank Act.

But based on recent CFPB trends, specifically its Aug. 11, circular deeming insufficient data protection or information security UDAAP, it is likely that the CFPB may view violations of

the contemplated privacy rule as a UDAAP.

A UDAAP may also trigger violations of state consumer protection laws with private rights of action that potentially could lead to consumer class actions as well.

It is also likely implementation of the proposed rule could also result in an increased risk of misconduct by third-party vendors and random bad actors.

As noted above, it is important for financial institutions and card issuers to maintain appropriate oversight over their vendors as this proposed rule will result in greater exposure for institutions that utilize third parties to house and facilitate the delivery of the data.

Like with previous CFPB resolutions, regulators may consider whether institutions utilized the appropriate level of oversight of third-party vendors including the veracity of data conveyed, the controls and procedures in place to safeguard the data and the future usage of the data, among other things.

Conclusion

Again, while the rule is still in its infancy and remains in the rulemaking process, participation in this process will help facilitate collaboration between the bureau rule makers and the industry.

If an aspect of the proposed rule is particularly unworkable, the issue can be brought to the bureau's attention and ideally the bureau can make the necessary changes to reflect the realities of the industry.

While the CFPB is not generally swayed by industry-based feedback, this is a key opportunity for improvement prior to implementation.

It is important that all stakeholders, including smaller financial institutions and third-party vendors that work with consumer banking institutions, are able to have a voice in this process so that the rule also accounts for the varied capabilities and resources of different types of institutions.

Denise Barnes, Brandy Bruyere and Molly McGinley are partners at Honigman LLP.

Honigman associate Jewel M. Haji contributed to this article.

[1] https://www.consumerfinance.gov/about-us/newsroom/cfpb-kicks-off-personal-financial-data-rights-rulemaking/.

[2] https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf.