Articles + Publications | December 27, 2022

Locke Lord QuickStudy: CFPB's Data Access Rulemaking ?Process: A Heads-Up to Covered Data Providers ?

Locke Lord LLP

WRITTEN BY

Tara L. Trifon | Kenneth K. Suh | Laura L. Ferguson

RELATED OFFICES

Hartford | Houston

On October 27, 2022, the Consumer Financial Protection Bureau ("CFPB") began the process needed to implement a much anticipated rule regarding section 1033 of the Dodd-Frank Act by releasing an outline providing initial information on the proposed rule.[1] Once implemented, any rule will significantly affect "covered data providers" and early awareness will help those entities best be prepared. This article discusses the process, the currently predicted parameters of the rule, and likely requirements for "covered data providers".

As set forth in the Outline,[2] the proposed rule would require financial service companies to provide consumers with greater access and control over their own data, including with third-parties upon authorization. The CFPB hopes that this rule will promote competition and innovation to benefit consumers, part of its statutory mandate. In order to accomplish this, the CFPB needs to balance things like data privacy and security with consumer choice and ease of access.

The first step in the CFPB's rulemaking process is to obtain input from small businesses pursuant to the Small Business Regulatory Enforcement Fairness Act of 1996, which is likely going to be a lengthy process. Next, the CFPB will publish the proposed rule and review any public comments received. Then the CFPB will issue the final rule, probably in 2024, which will include a date by which the relevant financial service companies must comply.

Regardless of when the rule is ultimately implemented, it is likely to have a significant impact on consumers, financial institutions, and the constantly emerging fintech companies. As a result, it is important that impacted organizations stay informed of these developments.

What type of entities will be affected by the proposed rule?[3]

At least in the beginning, the CFPB only intends to make the rule applicable to entities that fit the definition of a "financial institution" in section 1005.2(i) of the CFPB's Regulation E, or a "card issuer" as set forth in section 1026.2(a)(7) of the CFPB's Regulation Z. The CFPB refers to the relevant financial institutions and card issuers as "covered data providers."

Entities that fall under the covered data provider definition include banks, credit unions, or "other persons" that

hold consumer accounts and issue debit cards, credit cards, and prepaid cards. The CFPB explains that it focused on these data providers because they implicate consumers' payment and transaction data.

Interestingly, though, CFPB also notes that a covered data provider includes entities that issue an access device and agree to provide electrical fund transfer services, like mobile wallets and electronic payment products. Typically such data providers do not have as much information about the consumer transactions as the actual banks or credit unions.

What information would a covered data provider need to make available?[4]

The CFPB has identified a significant amount of information that it believes should be provided to a consumer and/or authorized third party. While a large portion of this information is likely already given to the customer through their account statements and/or other communications, the CFPB expressly included a category of information not typically provided through account statements.

The information that would be subject to disclosure falls into six categories:

1) Periodic statement information for settlement transactions and deposits;

2) Information regarding prior transactions and deposits that have not yet settled;

3) Information about prior transactions that are not typically shown on periodic statements or portals (such as card networks, ATM networks, automated clearing house networks, check-collection networks, and real-time payment networks);

4) Online banking transactions that the consumer has set up but have not yet occurred;

5) Account identity information (*e.g.* name, address, social security number); and

6) Additional miscellaneous information, including consumer reports from consumer reporting agencies, fees that are assessed against a consumer's financial account, any incentives that the covered data provider offers to consumers, and any security breaches that exposed the consumer's identity or financial information.

Some of the information that is not traditionally provided to consumers is included in category three above, such as the interbank routing of a transaction. The CFPB justifies the production of this information as it could be helpful to consumers as they try to resolve disputes with respect to fraudulent or erroneous payments. However, this benefit has to be weighed against the real possibility that the information may be considered trade secrets or otherwise confidential, and that compelling disclosure could also lead to increased privacy risks.

Covered data providers may have to make changes, whether technological or contractual in nature, to address the required disclosure of the information contemplated by the proposed rule. In addition, covered data providers should analyze whether disclosing some of this information (such as the reports from credit monitoring agencies) would subject the entity to the requirements of other statutes like the Fair Credit Reporting Act.

How does the CFPB contemplate the information would be provided?[5]

The CFPB is seeking input on the methods and circumstances in which a covered data provider would need to provide a consumer with direct access to the requested information, or where it needs to provide access to the third party's authorized representative. In both situations, the CFPB contemplates that the covered data providers would utilize information portals.

With respect to a consumer's request, the CFPB proposes that the information be made available through an entity's online financial account management portal. This would allow the covered data provider to reasonably authenticate the consumer's identity and reasonably identify the information requested. It would also allow the consumer to export the responsive information electronically. Indeed, the CFPB notes that the production of information to a consumer in a different format may be burdensome for the covered data provider if there are no limitations set.

For third parties, the CFPB identifies the two typical methods by which a data provider makes information available to third parties. One method is through the provider's online financial account management portal using the consumer's credentials. The other method is through a portal where third parties do not need those credentials but the information is generally provided on an automated basis using screen scraping. While the latter method may have some limitations and poses some risks to consumers, the CFPB believes that creating a third-party access portal that does not require the third-party to have access to the consumer's credentials would enhance privacy and data security, as well as data accuracy. The CFPB also notes that some entities have started developing and implementing third-party access portals already, but the CFPB still intends to establish a framework so that standards and guidelines can develop consistently across the industry.

How would a consumer give authorization to release information to a third-party?[6]

The CFPB's proposal seems similar to the Health Insurance Portability and Accountability Act of 1996, as amended (the "HIPAA"), which prevents a health care provider from providing health-related information to a third-party without receiving a release form that specifically identifies what information can be provided, and to whom.

Under the CFPB's proposed rule, a covered data provider would only have to respond to a request to share data with a third-party after receiving evidence of the third-party's authority to access the information. The CFPB would require that the third-party provide the consumer with an "authorization disclosure" that would obtain the consumer's informed and express consent as to the access terms. This disclosure would also require the third-party to certify that it will abide by certain obligations regarding the collection, use, and retention of the consumer's information.

How would the third-party's use of the information be limited?[7]

The CFPB is considering limiting the third-parties' use of the consumer's information beyond what is reasonably necessary to provide the product or services that the consumer has requested. This may include limiting the third-party's use of the consumer data and/or sharing the data with other business related entities. The various approaches that the CFPB is contemplating includes prohibiting: (1) all secondary uses, (2) certain high risk secondary uses, (3) any secondary uses unless the consumer opts into those uses, and (4) any secondary use if

the consumer opts out of those uses.

Will there be any additional data security requirements imposed on data providers or third parties?[8]

The CFPB believes that all, or almost all, of the covered data providers are likely already obligated to comply with the requirements of the Gramm-Leach-Bliley Act ("GLBA"). As such, the proposed rule does not include any additional data security requirements on covered data providers.

However, the CFPB is considering whether specific data security standards should be imposed on authorized third-parties. Such standards could include requiring the third-parties to develop, implement, and maintain a written data security program appropriate to the third parties' size and complexity, as well as appropriate to the volume and sensitivity of the relevant consumer information. Another possibility is that the CFPB requires the authorized third-parties to comply with the Safeguards Rule or Safeguards Guidelines of the GLBA.

Are there any obligations relating to data accuracy?[9]

The CFPB has included requirements for both covered data providers and authorized third-parties to confirm that the data requested and provided is accurate. With respect to the authorized third-parties, the CFPB seems to base standards on other relevant laws, such as the Fair Credit Reporting Act or other state privacy laws. In particular, the CFPB proposes that third-parties "maintain reasonable policies and procedures to ensure the accuracy of the information that they collect and use to provide the product or service the consumer has requested, including procedures relating to addressing disputes submitted by consumers." This could result in a high burden on the third-parties. In addition, there is the possibility that the "reasonable policies and procedures" could mean different things, depending on the jurisdiction.

Similarly, the CFPB proposes that covered data providers also implement reasonable policies and procedures to ensure data accuracy. The CFPB also contemplates that these policies and procedures would establish performance standards, and prohibit the providers from conduct that would adversely affect the accurate transmission of consumer information.

The Takeaway

While any final rule will probably not be issued and/or effective until 2024, those companies that have consumer financial data, or share such data, should consider the CFPB's outline and consider how they can satisfy the expected standards. In the interim, we will continue to monitor the CFPB's rulemaking process, including any input obtained from small businesses, the proposed rule, and any public comments received.

—

[1] Section 1033(a) of the Dodd-Frank Act authorizes the CFPB to prescribe rules requiring: "a covered person [to] 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."

[2] Small Business Advisory Review Panel For Required Rulemaking on Personal Financial Data Rights

[3] Outline, at § III.A.

[4] Outline, at § III.C.

[5] Outline, at § III.D.

[6] Outline, at § III.B.2.

[7] Outline, at § III.E.

[8] Outline, at § III.E.2.

[9] Outline, at § III.C.?

RELATED INDUSTRIES + PRACTICES

- Financial Services
- Financial Services Litigation
- Privacy + Cyber