POLSINELLI | What a law firm should be.™

Analyzing the CFPB's Personal Data Financial Rights Rule: What You Need to Know

The Consumer Financial Protection Bureau (CFPB) published a proposed **Personal Financial Data Rights rule** (the "Rule") last week. Once finalized, the Rule will implement requirements relating to consumer rights set forth in the Dodd-Frank Act. More specifically, the Rule will provide consumers with broad rights to access and control the disclosure of their personal information held by financial institutions that provide checking, savings, or other prepaid accounts to consumers for individual or household purposes, as well as credit card and digital wallet providers ("financial institutions"). The Rule will represent an increase in such institutions' obligations regarding data access and portability, as these institutions have had limited obligations under the various state-level privacy laws enacted over the past few years due to exemptions for data or entities subject to the Gramm-Leach-Bliley Act (GLBA), which has traditionally governed financial institutions' obligations with respect to data privacy.

Key Requirements under the Rule

The Rule imposes several key requirements on financial institutions:

Access Rights

Subject to limited exceptions specified in the Rule, Financial institutions must make available to consumers, or authorized third parties (at the consumer's request), the most current version of "covered data" it possesses regarding the applicable consumer. "Covered data" includes the following:

- Historical transactional information covering the 24-month period prior to the date of the request (if the consumer has had a relationship with the institution for such period, and for the duration of the relationship if less than 24 months).
- Current account balances.
- Information necessary to initiate payment to or from a checking, savings, or prepaid account (e.g. routing and account numbers, which may be tokenized as appropriate).
- The terms and conditions relating to a consumer's use of the applicable financial product or service (e.g. fee schedules, interest rates, rewards program terms, and whether the consumer has entered into an arbitration agreement).
- Upcoming bill information (including any payments to third parties scheduled through the financial institution).
- Demographic information necessary to verify an account.

Interface Requirements

Financial institutions must provide separate interfaces for both consumers and their authorized third parties to provide access to the information described above. In addition, upon a consumer or authorized third party's specific request, a financial institution must make available covered data in a machine-readable format. Notably, financial institutions *may not* charge any fees in connection with either the establishment or maintenance of the required interfaces or in

receiving and responding to requests for data pursuant to the Rule.

The interfaces used to process requests must either comply with designated industry standards or otherwise meet standards widely used in the financial industry. The CFPB has proposed specific performance and security requirements, which notably include successful response rates, response times (less than 3,500 milliseconds), access cap prohibitions, and obligations to meet the information security requirements established under the GLBA.

Requirements for Authorized Third Parties

Third parties may request covered data from financial institutions solely to the extent a consumer has provided express authorization in writing or electronically pursuant to a clear and conspicuous request for such authorization that is segregated from all other material. The request must clearly identify the third party's name, the name of the financial institution, the product, or services that the consumer has requested the third party to provide, the data to be collected, and a description of the mechanism for the consumer to revoke the foregoing authorization.
Such third parties can only use the information they receive to provide the products or services described in the authorization and may not use the information for their own purposes, including for advertising or to sell the information.

Authorizations are only effective for one year and must be renewed annually in accordance with the above requirements. Further, such authorizations may be revoked at any time. If revoked, the third party must notify the financial institution and cease any further requests for the covered data.

Like financial institutions, authorized third parties must comply with the GLBA's information security requirements.

Compliance Timeframes and Next Steps

As noted above, the CFPB proposed the Rule on October 19, 2023. It is soliciting comments on the Rule through December 29, 2023. Given the proposed requirements, it is likely that both advocates and opponents of the Rule will provide substantial comments, which may result in a long gap between the end of the comment period and the publication of the final version of the Rule. Pending any changes in response to these comments, the Rule phases in compliance based on the size of financial institutions, with the largest institutions required to comply within six months of publication of the final rule, and extended timeframes for smaller institutions.
Given the substantial requirements, financial institutions can begin to work toward compliance by taking the following steps:

- Commencing or updating any data cataloging or mapping exercises to facilitate the processing of requests for covered data.
- Begin budgeting of financial and personnel resources for the implementation and maintenance of the interfaces, especially if the prohibition on fees remains in the final version of the Rule.
- Begin work on the creation of policies and procedures, including security protocols, designed to meet the Rule's requirements and establish a plan for the implementation of these policies.

If you're interested in providing comments for the proposed rule, you can do so through Polsinelli. Please contact **Liz Harding**.