CADWALADER

Cabinet **News and Views**

Informed analysis for the financial services industry

Technology and Other Obligations for the CFPB's Personal Data Financial Rights Rule, Part 3

By **Mercedes Kelley Tunstall**
Partner | Financial Regulation

In our continuing series on the proposed rule introduced by the Consumer Financial Protection Bureau ("CFPB") regarding Personal Data Financial Rights, this week's installment examines the obligations that are applicable to all entities subject to the rule. For an overview of the proposed rule, please see our first post, and to understand the entities that are subject to the rule, please see our second post.

Also, consider the CFPB's new proposed rule involving a Larger Participant rulemaking wherein the CFPB defines the "digital wallet and payment app" space (*e.g.*, Apple Pay, Google Pay, Cash App) as a financial market and thereby seeks to declare that providers of such services, including BigTech firms, as being subject to CFPB supervision and, of course, all consumer financial services laws and regulations. There is an accompanying article in this week's Cabinet issue, providing further details on that Larger Participant rulemaking.

For reference, the Personal Data Financial Rights proposed rule is available here and the overall Federal Register notice is available here. Comments are due December 29, 2023.

As we discussed last week, there are three groups of entities that are subject to separate sets of requirements under this proposed rule (again, see more discussion about the details of these groups in our post from last week):

- data providers, which are entities that have covered data in their control or possession concerning a covered consumer financial product or service that the consumer obtained from that entity;
- authorized third parties, which are those entities who "seek access to covered data from a data provider on behalf of a consumer" so that they can provide a product or service the consumer requested; and

- data aggregators, which are those entities that are "retained by and [that provide] services to the authorized third party to enable access to covered data."

Two definitions are important to understand the obligations discussed below. First, a covered consumer financial product or service includes all payment cards, whether the cards are debit cards, credit cards or prepaid cards, as well as all electronic payment accounts and transfers that are governed by Regulation E, and all products or services that "facilitate payments from a Regulation E account or Regulation Z credit card."

Second, "covered data" includes all of the following: transaction data; account balance; information needed to initiate payment to or from a Regulation E account (which can be tokenized or non-tokenized); terms and conditions governing the covered consumer financial product or service; upcoming bill information; and basic account verification information (name, address, email address and phone number associated with the covered consumer financial product or service).

There are some exceptions for the provision of covered data: The data provider need not provide such data (1) when it includes information that is "confidential commercial information," meaning that it is a custom credit score or other kind of risk or predictive designation; (2) when the information is "collected by the data provider for the sole purpose of preventing, or detecting, fraud or money laundering, or making any report regarding other unlawful or potentially unlawful conduct"; (3) when the information is confidential according to other provisions of law, but not when it is deemed confidential due to privacy policies; or (4) when the data cannot be retrieved in the "ordinary course" of business.

Most entities providing comments upon the proposed rule will likely address the elements of covered data, asking for more clarification on the scope of each element of the covered data definition, and particularly focusing upon the third exception, which seems incongruent with the purpose of many privacy laws in effect that incorporate open-ended definitions of data that may be deemed sensitive and confidential, leaving each entity to define in its privacy policy that data that should be deemed sensitive and confidential based upon the industry and circumstances of the generation, collection and use of that data.

Data providers have many obligations under the proposed rule, with the primary obligation being to "*make available to a consumer and an authorized third party, upon request, covered data in the data provider's control or possession concerning a covered consumer financial product or service that the consumer obtained from the data provider, in an electronic form usable by consumers and authorized third parties*." The covered data that must be made available should be the most recent covered data, including data regarding transactions that have been authorized, but that have not yet been settled.

The means by which the data provider must make this information available is through a "consumer interface" that provides consumers with "machine readable files" and a "developer interface" that presents the information in a standardized format. Data providers may not charge fees for access to, development or maintenance of, these interfaces. The consumer interface is intended to allow consumers to request their own data, the developer interface is intended to allow

the data to be accessed by authorized third parties. The proposed rule details the process around establishing the "standardized format" of covered data and appears to be encouraging the industry to work amongst itself to develop these standards. Until such time that a standard format has been defined by industry, then the data provider must benchmark with other data providers and provide information in a fashion similar to how its peers provide that data to be deemed in compliance with this obligation. Data providers must also maintain commercially reasonable "up times" for the interfaces and may not impose an "access cap" to prevent authorized third parties from checking on the data as often as they like. Despite that access-cap prohibition, the data provider may prevent access to the data for risk-related reasons and because there is insufficient information to ascertain which data is being accessed. These interfaces also must employ authentication protocols in keeping with the rule's requirements, which on the developer interface includes not only authenticating the authorized third party, as well as the consumer, and the scope of the consumer's authorization to the authorized third party, but also provides a mechanism by which consumers can inform the data provider that they no longer authorize access to their data by an authorized third party that had previously been given authorized access.

When combined with aggressive compliance dates targeted to the largest of financial institutions, which have the most complex and, often, the most intransigent systems, comments from data providers are likely to be very focused upon the operational, technological and practical aspects of these requirements in the proposed rule, as well as to make forceful cases regarding the need to have some number of years to implement these requirements in full. Under the provision of the CFPA that the CFPB is using to support this rulemaking, the CFPB is supposed to remain technology-agnostic and avoid imposing rigid technology requirements on the affected entities. Accordingly, the comments on these requirements are likely to also point out when the prescriptions are too rigid for a technology-agnostic stance.

Authorized third parties, as we discussed last week, are primarily required to obtain express informed consent from the consumer, pursuant to a defined authorization that designates the name of the authorized third party; the name of the data provider; a description of the product or service being requested by the consumer from the third party; a statement that the data accessed will only be collected, used and retained for the purpose of providing the product or services; the categories of covered data that will be accessed; a certification; and a description of the method for the consumer to revoke authorization from the third party. Authorizations must be renewed at least annually. However, the biggest concern for authorized third parties is likely the prohibition on incorporating any form of targeted advertising or cross-selling of other products or services into the process of interacting with the consumer.

Finally, data aggregators must work hand-in-hand with the authorized third parties, under the proposed rule. They must be named and included in the authorization provided to the consumer, and must certify to the consumer that the covered data being accessed will only be used for the purposes identified by that authorized third party. Practically speaking, many companies offering services that would typically be viewed as data aggregation will likely be deemed authorized third parties for purposes of this proposed rule.

Stay tuned next week for a final installment on the Personal Financial Data Rights proposed rule, which will address some topics not already discussed and will highlight the areas we think will face the most friction between actors in the industry and between the industry and the CFPB.
