CADWALADER

Cabinet **News and Views**

Informed analysis for the financial services industry

CFPB's Personal Financial Data Rights Proposed Rule, Part 4

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

This final installment of our coverage on the Consumer Financial Protection Bureau's proposed rule regarding "personal financial data rights" builds upon concepts and concerns covered in our earlier posts. For an overview of the rule, read our first installment. To understand what entities would need to comply with the proposed rule, read our second installment. To better understand the obligations and technology requirements of the proposed rule, read our third installment.

As promised, this fourth and final installment picks up on a few issues not already discussed and highlights portions of the proposed rule that are likely to cause great conflict and consternation for the entities subject to the rule. First, and this is an issue that is ripe for conflict, is the compliance timelines included in the proposed rule. As ever, the CFPB continues to push for aggressive compliance timelines and to default on pushing the largest institutions to comply with the proposed rule first. In this case, the proposed rule requires full compliance for the largest data providers (*i.e.*, depository institutions that hold at least $500B and nondepositories that generated at least $10B in revenue) within six months of the final rule being published; one year for smaller data providers (*i.e.*, depository institutions that hold at least $50B, but less than $500B or nondepositories that generated less than $10B); and then two-and-a-half years ($850MM, but less than $50B) and four years (less than $850MM) for the smallest depository institutions. There are no timelines for compliance given for the "authorized third parties" and the "data aggregators," indicating that the data provider institutions are expected to drive compliance by requiring these third parties to meet the new standards, reporting and protocols.

The author has spent many years working with a wide variety of financial institutions over the years on technology-related issues, and is only too aware of how changing technology requirements, especially technology requirements relating to the collection, maintenance, reporting and use of protected information requires a lot of time to get right. Six months to completely change the handling of

information designated as “covered data” according to this rule is an impossible timeframe, even just for internal changes, much less when the financial institution will have to ensure that third parties change how they do business to accommodate that financial institution’s need to comply with the law. For most financial institutions, but particularly the largest financial institutions, the sheer number of systems, databases and processes that would need to be involved in the changes contemplated by the proposed rule is daunting. The reason that the largest financial institutions have the greatest number of systems affected is due to the persistence of legacy systems in their system architecture. (Indeed, at one point along the way, the author worked with a financial institution that was managing its account records via a souped-up version of airline reservation software from the 1970’s. Several systems had been built like scaffolding around that core system, of course.) Without getting into too much technical discussion, the reason legacy systems persist is often because the amount of downtime and costs related to completing transition from that legacy system are both astronomical and operationally inconceivable. And the largest financial institutions are the ones that are most likely to have the most complex architectures that include multiple sets of legacy systems and their adjacent scaffolding. To this observer, even with their impressive resources, the largest financial institutions will not be able to meet a year-long compliance timeframe, much less a six-month compliance requirement.

Reasonable minds may question whether the technology changes needed internally to comply will actually be all that difficult. After all, financial institutions have been made to comply with privacy laws for many years and imposing a new set of requirements upon the disclosure and sharing of protected information should be expected and anticipated. At this point, it is useful to delve into the scope of “covered data” for purposes of the proposed rule. Covered data includes those data elements that are standard fare from a privacy perspective, including name, address, email address, phone number, and account number. However, the definition of covered data in the proposed rule also includes information that is not typically covered by privacy laws, such as the terms and conditions of products and services the customer has obtained, including fee schedules and whether the consumer has opted into overdraft coverage or opted out of an arbitration agreement. Further, the definition of covered data also extends to transaction-level information and tokenized account information, both of which may be accessed by third parties today, but only under the auspices of privacy policies maintained by those third parties and enforced against the third parties by the consumer, not under the financial institution’s own privacy policies and privacy and security-related obligations. The CFPB’s proposed rule therefore has the added dimension of increasing a financial institution’s privacy and security obligations and exposures under other laws, including, but not limited to, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act and the Authentication Guidance from the Federal Financial Institutions Examination Council (“FFIEC”).

Layering on top of the “strange bedfellow” data elements in the definition of covered data are two additional issues that are likely to rankle the industry. First, is the proposed rule’s requirement that zero fees be charged to customers for providing this information. The CFPB has been very clear under the Biden administration that fees of any kind charged by banks for the services they provide in the retail sector are viewed suspiciously at best, and at worst, should not be charged at all. Thus, the proposed rule’s ban on fees is not unexpected. But given

the scope of the proposed rule and the work that financial institutions must do internally and externally vis a vis the authorized third parties and data aggregators, banning fees outright is pouring salt in the wound. Second, the proposed rule prohibits financial institutions from limiting the number of times an authorized third party can request data except when the denial is reasonably related to risk management concerns, meaning "at a minimum, [the denial must] be directly related to a specific risk of which the data provider is aware, such as a failure of a third party to maintain adequate data security." According to this characterization of what is "reasonable" a generic denial of requests for data that exceed a certain volume over time, such as the kinds of problems that lead to DDOS attacks, would not be sufficiently reasonable because it is not tied to a "specific risk" predicated upon knowledge the financial institution has of the requesting authorized third party. Even if the requests fall short of a DDOS attack, but are persistent and frequent – with authorized third parties refreshing their information every minute of the day, 24/7, for example – accommodating such volumes will require an extremely robust interface and intense security controls, all the more reason why there is likely to be much pushback regarding the proposed rule's short compliance timeframes.

These points of conflict aside, the CFPB's proposed rule presents an innovative framework for fostering an environment where consumers can freely move between financial service providers, a concept called "open banking" that gives consumers meaningful control over their data and allows them to "walk away from bad service." By conceiving of categories for each participant in the open banking environment, the proposed rule introduces definitions and roles that have not been well articulated previously, but may now be used to help drive conversations and innovations.
