OVERVIEW OF THE CFPB'S OPEN BANKING PROPOSAL

On October 19, 2023, the Consumer Financial Protection Bureau (**CFPB**) issued a proposal on Personal Financial Data Rights (**Proposed Rule**), which implements section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (**Section 1033**) and accelerates a shift to open banking in the United States. This is a meaningful development as the United States catches up to other jurisdictions around the world, including e.g., Europe and Australia, where open banking regulations came into force in 2019. Comments to the Proposed Rule are accepted through December 29, 2023, and the CFPB intends to finalize the regulation by Fall 2024.

The Proposed Rule, similar to other open banking regulations, sets out a framework to govern consumer access to financial data through Application Programming Interfaces (**APIs**) and outlines related requirements for financial institutions and other actors who handle such data. Central to the Proposed Rule are the themes of consumer consent and control over financial data; stringent security measures for covered data in transit and at rest; standardized, secure and interoperable APIs; broader competition and innovation within the financial sector; and regulatory oversight to ensure appropriate management of opportunities and risks.

COVERED ENTITIES

Section 1033 requires that a covered person makes available to a consumer, upon request, information in such person's control or possession concerning the financial product or service the consumer obtained from such person, including transaction, cost and account information. In implementing these requirements, the Proposed Rule aims to regulate three categories of entities:

- **Data providers** – financial institutions, card issuers, and other persons with control or possession of information regarding a covered consumer financial product or service.
- **Authorized third parties** – entities that have satisfied authorization requirements under the Proposed Rule and seek access to data from a data provider on behalf of a consumer to furnish a requested product or service (including competing financial institutions).
- **Data aggregators** – entities retained by authorized third parties to access covered data on behalf of a consumer.

COVERED FINANCIAL PRODUCTS AND SERVICES AND COVERED DATA

Under the Proposed Rule, the scope of covered consumer financial products or services would initially be limited to "Regulation E accounts" and "Regulation Z credit cards," as those terms are defined under these regulations, as well as the facilitation of payments from a Regulation E account or a Regulation Z credit card. CFPB intends to address additional financial products or services over time.

Covered data includes transaction information; the consumer's account balance; information to initiate a payment; account terms and conditions; upcoming bill information; and account verification information. Covered data excludes confidential commercial information; information collected to prevent fraud or money laundering or to detect unlawful conduct; information required to be kept confidential under applicable law; and information that is not retrievable in the ordinary course.

REQUIREMENTS FOR DATA PROVIDERS

The Proposed Rule would require data providers to develop and maintain consumer interfaces and developer interfaces to enable consumers to request and timely receive "the most recently updated covered data", subject to specific information security requirements and performance parameters, including response times. Relatedly, the Proposed Rule would impose limitations on data providers' collection, retention and use of covered data.

Under the Proposed Rule, data providers would be prohibited from allowing a third party to access a data provider’s developer interface by using consumer credentials. Thus, the Proposed Rule would prohibit so-called "screen scraping" where a third party uses a consumer's log in credentials to access a financial institution's online banking to automatically "scrape" information. Data providers would be required to make covered data available in a machine-readable, standardized format and would also have to disclose documentation, including metadata describing all covered data and their corresponding data fields, and other documentation sufficient for a third party to access and use a data provider's developer interface.

Data providers would be prohibited from charging consumers or authorized third-parties fees to pay for consumers' requests. At the same time, data providers can expect to incur significant expenses to comply with the Proposed Rule.

REQUIREMENTS FOR AUTHORIZED THIRD PARTIES AND DATA AGGREGATORS

Under the Proposed Rule, a consumer must provide an express informed consent before a party becomes an authorized third party. This requires a signed authorization disclosure that contains certain detailed descriptions and certifications. A consumer may revoke a third party's access to covered data, including for a particular product or service while continuing to allow the same third-party access for a separate product or service. A data provider may deny a third-party access to covered data based on reasonable risk management concerns.

Once authorized, these parties would be subject to specific obligations relating to covered data, including restrictions on collection, use and retention; information security requirements; communication requirements; revocation requirements; and requirements to maintain reasonable policies and procedures to ensure compliance. Notably, under the Proposed Rule, covered data cannot be used for any purpose other than what is "reasonably necessary" to provide the consumer with a financial product or service. This secondary use prohibition would likely significantly impact a number of entities.

If an authorized third party uses a data aggregator, the aggregator would become subject to the same obligations. The aggregator's identity would have to be disclosed in the authorization document signed by the consumer.

IMPLEMENTATION TIMELINE

Data providers would be required to comply with a final rule, once issued, on a staggered schedule based on asset and revenue thresholds and entity type. The compliance window ranges from 6 months to 4 years from the date the final rule is published in the Federal Register.

CONTACTS

Philip Angeloff
Counsel

T +1 202 912 5111
E philip.angeloff
@cliffordchance.com

Inna Jackson
Tech Knowledge &
Innovation Attorney

T +1 212 878 3292
E inna.jackson
@cliffordchance.com

Young Kim
Counsel

T +1 212 878 4902
E young.kim
@cliffordchance.com