KRIEG DEVAULT

Insights

CFPB Issues Final Rule on Open Banking

November 11, 2024

By: Brett J. Ashton and Alexus D. Lucas

On October 22, 2024, the Consumer Financial Protection Bureau (the "CFPB") released its final rule (the "Rule") on Personal Financial Data Rights under Section 1033 of the Consumer Financial Protection Act. The Rule requires data providers to make consumer's covered data electronically available to the consumer and authorized third parties, free of charge, at the consumer's request. The purpose of the Rule is to give consumers more agency over their financial data and promote competition by allowing consumers to shop for better rates and terms more easily among financial product service providers.

Who is a Covered Data Provider?

The Rule defines a covered data provider to include: (1) a financial institution as defined in Reg. E (12 C.F.R. § 1005.2(b)); (2) a card issuer as defined in Reg. Z (12 C.F.R. § 1026.2(a)(15)(i)) or; any other person that controls or possesses information concerning a covered consumer financial product or service that the consumer obtained from that person. While depository institutions are considered covered data providers, the Rule provides an exemption for depositories with total assets equal to or less than the SBA size standard as codified in 13 C.F.R. § 121.201, which is currently $850 million. The total assets held by a depository institution are determined by averaging the assets reported on its four preceding quarterly call report submissions to the Federal Financial Institutions Examination Council or National Credit Union Association.

What is a Covered Consumer Financial Product or Service?

The following are considered covered consumer financial products or services: (1) an account as defined in Reg. E (12 C.F.R. § 1005.2(b)); (2) a credit card as defined in Reg. Z (12 C.F.R. § 1026.2(a)(15)(i)); or (3) payment facilitation from a Reg. E account or Reg. Z credit card, excluding products or services that only serve to facilitate first-party payments.

What Information is Covered Data?

Covered data is data from a covered consumer financial product or service, and includes:

- Transaction information, including at least 24 months of historical transaction information in the data provider's control or possession – this includes transaction amount, transaction date, payment type, pending or authorized

status, payee or merchant name, reward credits, and fees or finance charges;
- Account balance information;
- Information to initiate payment to or from a Reg. E account directly or indirectly held by the data provider, provided the data provider also directly or indirectly holds the underlying Reg. E account;
- Terms and Conditions that illustrate the legal obligation between the data provider and the consumer;
- Upcoming bill information; and
- Basic account verification, limited to the name, address, email address, phone number, and an account identifier if applicable.

What Covered Data Does Not Have to Be Disclosed?

Data providers are not required to provide the following information:

- Confidential commercial information;
- Information collected solely for the purpose of preventing fraud or money laundering, or detecting and reporting potentially unlawful conduct;
- Information required to be kept confidential by other laws; and
- Information not retrievable in the ordinary course of the data provider's business.

Compliance Requirements for Covered Data Providers

Covered data providers must make covered data available in a usable electronic format at no charge to consumers and authorized third parties upon request. Covered data providers must:

- Maintain a consumer interface and a developer interface for the purposes of receiving, processing, and responding to requests for covered data;
- Upon request by a consumer or authorized third party, make covered data available in a standardized and machine-readable format that can be retained and transferred for processing into a separate information system;
- Make available the most recently updated covered data that it has in its control or possession at the time of a request, including information concerning authorized but not yet settled transactions;
- Establish written policies and procedures for requesting covered data that are appropriate relative to the size, nature, and complexity of the data provider's activities;
- Disclose information necessary to facilitate access to covered data, including (1) its legal name and any assumed name used in doing business with the consumer, (2) a link to its website, (3) its legal entity identifier (LEI), and (4) appropriate contact information for questions about accessing covered data; and
- Refrain from taking any action with the intent of circumventing the Rule's disclosure requirements, such as rendering the covered data unusable before providing it or adopting processes that materially discourage a consumer or authorized third party from accessing the covered data.

What are the responsibilities for authorized third parties?

Authorized third parties also have distinct obligations under the Rule. Third parties seeking access to covered data on the consumer's behalf to provide a product or service the consumer requested must provide the consumer with authorized disclosures in written form and obtain the consumer's express written consent to access covered

data on the consumer's behalf via the authorized disclosure. The authorized disclosure must contain required terms and restrictions on data access defined in new 12 C.F.R. § 1033.411(b) and a statement certifying the third party's agreement to comply with the Rule. Authorized third parties may rely on data aggregators to facilitate access to covered data, but the authorized disclosures must then also identify the name of the data aggregator and include a statement certifying to the consumer that the data aggregator will comply with the Rule as well.

The Rule also restricts the third party's collection, use, and retention of covered data to only that which is reasonably necessary for providing the requested product or service and for up to one year after the date of authorization. For example, accessing and retaining covered data for the purpose of targeted advertising, cross-selling, and the sale of covered data would not be within the scope of what is reasonably necessary to provide a requested product or service.

Finally, authorized third parties are also required to develop a set of policies and procedures to confirm the accuracy of the covered data they receive; verify their systems for maintaining covered data have adequate data security programs; facilitate consumers' access to information regarding the third party's access to their covered data; and ensure retention of any records that demonstrate their compliance with the requirements with Subsection D of the Rule.

When will covered data providers be expected to comply?

Compliance dates for covered data providers are staggered based on asset size, beginning on April 1, 2026 for depository institutions with at least $250 billion in total assets and non-depository institution data providers that generated at least $10 billion in total receipts in either calendar year 2023 or calendar year 2024; April 1, 2027 for depository institutions with at least $10 billion in total assets but less than $250 billion, and non-depository institution data providers that generated less than $10 billion in total receipts in either calendar year 2023 or calendar year 2024; April 1, 2028 for depository institutions with at least $3 billion in total assets but less than $10 billion; April 1, 2029 for depository institutions with at least $1.5 billion in total assets but less than $3 billion, and; April 1, 2030 for depository institutions with at least $850 million in total assets but less than $1.5 billion.

However, within hours of the Rule being released, the Kentucky Bankers Association and the Bank Policy Institute filed suit against the CFPB in federal court seeking to set aside the Rule and enjoin its implementation. The court is yet to schedule a preliminary hearing in the matter, styled as Forcht Bank, N.A., Kentucky Bankers Association, and Bank Policy Institute v. Consumer Financial Protection Bureau and Rohit Chopra, in his official capacity, Case No. 5:24-cv-00304-DCR (E.D. Ky. filed Oct. 22, 2024). While the outcome of this litigation is uncertain, financial institutions should begin to review their data processes to assess their readiness to comply with the Rule.

Krieg DeVault's Financial Institutions attorneys are monitoring developments in this area of law, and able to assist your institution in its preparations in the event the Rule becomes effective.
