BCLP. Client Intelligent

Insights

OPEN BANKING: WHEN YOU BUILD IT, WILL THEY COME?

CFPB PROPOSES RULES REQUIRING BANKS TO SHARE CONSUMER DATA

Nov 03, 2023

SUMMARY

The federal consumer protection agency's proposed rule would give consumers greater control over access to their personal financial information held by banks and credit unions. The CFPB's stated goal is to increase competition in consumer banking by making it easier, less costly and safer for consumers to move their banking relationships to competing banks, credit unions and fintechs.[1] The rule comes thirteen years after it was expressly mandated in the Dodd-Frank Act.[2]

WHAT THE PROPOSED OPEN BANKING RULE DOES

Under regulations proposed October 19th by the Consumer Financial Protection Bureau[3], Banks must share a consumer customer's data with third parties when directed by the consumer. The proposed Personal Financial Data Rights rule (the "Open Banking Rule") covers checking, prepaid accounts, credit card accounts and digital wallets. The rule would not apply initially to mortgages, car loans and student loans. Banks must make data available through APIs and may not charge for such access. The consumer's opt-in authorization of access for a third-party provider would expire after each year unless the consumer renews the authorization. Recipients of the data may use the data only for purposes reasonably necessary to provide the specific products for which the consumer authorized access. Consumers may revoke permission at any time and the data recipients must delete the consumer's data when permission is revoked. Recipients would be prohibited from using covered data for other commercial purposes without the consumer's consent, such as for targeted marketing, behavioral advertising or sale of the consumer's data. Large banks must comply within six months of publication of the final rule while smaller depository institutions are given from one to four years to comply, depending on size. Banks and credit unions that do not provide online consumer interfaces are exempt from compliance. Comments on the proposed rule must be submitted by December 29, 2023.

While consumer advocates and industry participants will find many issues in the proposal upon which to comment before the rule is finalized, the most substantial obstacle to timely implementation and realization of the CFPB's goals may be the designed ambiguity as to a specific

technical standard for data access, as described below. While the proposed permission to use existing recognized standards may hasten deployment by data providers, the lack of specification in the rule may give rise to prolonged market uncertainty as to which standard should be used, and force potential data users to accommodate multiple "standardized" formats.

WHAT THE PROPOSED RULE DOES NOT DO

Although the proposed rule includes measures to discourage access to consumers' data pursuant to current credential-based screen-scraping practices, it does not clearly prohibit such practices. The statutory authorization for the proposed rule also does not prohibit continued usage of current methodologies. Instead, the CFPB's proposes to make available a more reliable and secure pathway to provide consumers access to their data and convenient usage via third parties who offer competitive and innovative services. The Open Banking Rule requires covered data providers to make certain data available through APIs and establishes elaborate requirements to qualify third parties to access the data on behalf of a consumer. It does not prohibit third parties from accessing that data through current practices without meeting the elaborate requirements for access by using the newly mandated API.[4]The result is that while the institutions that currently hold a consumer's data are required to make costly investments to facilitate secure, comprehensive and timely access to the data without charge, the Open Banking Rule does not appear to require current data users to make the corresponding investments to migrate to the mode of access that data providers would be required to provide. Further, it appears that the rule is intended to facilitate fintech services that would access data held by the consumer's existing depository on a transaction-by-transaction basis rather than addressing transfers of data and funds to facilitate a consumer's transfer of its depository and payment card relationships to an alternative bank or credit union. For example, a data provider is permitted to provide tokenized routing and account data to facilitate funds transfers from a "Reg E account," which could effectively limit transactional services to the institution that can utilize the tokenized data. However, as mentioned below, the CFPB notes in its explanatory notice that the rule is not meant to preclude a consumer's access to historical data. These limitations on the functionality supported by the proposed regulation do not arise from the wording of the statutory mandate, which provides that a covered institution must

> "make available to a consumer, upon request, information in the control or possession concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data."[5]

Finally, the proposed rule only addresses access to data and does not address transfers of funds, leaving funds transfers and payments that might be executed through the authorized third party's services to existing rules and processes. Funds transfers and payments are outside the scope of the provisions of the Dodd-Frank Act that would be implemented by the proposed Open Banking Rule.

COVERAGE

A "data provider" that must comply with the Open Banking Rule is an organization that controls or possesses certain "covered data" concerning a "covered consumer financial product or service."[6]Covered consumer financial service or products are: (1) accounts as defined in Regulation E (12 CFR 1005.2(b)); credit cards as defined in Regulation Z (12 CFR 1026.2(a)(15)(i)); and a service that facilitates payments from a Regulation E account or Regulation Z credit card.[7]The reference to facilitating payments is intended to extend coverage to "all consumer-facing entities involved in facilitating the transactions the CFPB intends to cover."[8]A data provider is defined as an organization (or service provider affiliate) that markets or provides a consumer product or service that is a financial institution under Reg E, a card issuer under Reg Z or that otherwise controls or possesses covered information obtained from a consumer.[9]The Open Banking Rule would exempt depository institutions that do not provide a consumer interface.[10]"Consumer interface" means "an interface that a data provider maintains to receive requests for covered data and make available covered data in an electronic form usable by consumers in response to the requests."[11]

COMPLIANCE DATES – "APPROXIMATELY"

Six months after publication of the final rule (approximately Q4 2024):

- Depository institutions with assets greater than $500 billion or
- Non-depository institutions with revenues greater than $10 billion

One year after publication of the final rule:

- Depositories with assets greater $50 billion, and
- Non-depository institutions with less than $10 billion in revenues

2½ years after publication of the final rule:

- Depositories with assets greater $850 million

Four years after publication of the final rule:

- Depositories with less than $850 million in assets.

"Total assets" refers to the amount "based upon the total consolidated assets of the institution as reported in published financial statements, as used by the FFIEC."[12]

The NPR does not explain why deadlines are "approximate" but recognizes varying obstacles that covered depository data providers would face in complying with the Open Banking Rule:

> "[T]he CFPB understands that a number of factors may affect how quickly a data provider could comply with the proposed rule. These include, for example, a data provider's size, relative technological sophistication, use of third party service providers to build and maintain software and hardware systems, and, in the case of many data providers, the existence of multiple legacy hardware and software systems that impact their ability to layer on new technology. Many smaller depository data providers will need to rely on cores and other third party service providers to create interfaces required by the proposed rule. These entities may experience significant wait times since many other entities may be relying on the same providers for the development of their interfaces. If a depository institution data provider builds its own interface without the assistance of a third party service provider, it may need additional time to do so."[13]

The CFPB is less accommodating to fintechs:

> "The CFPB preliminarily believes nondepository data providers do not have the same obstacles with respect to compliance as depository institutions because they do not have as many vendors and information technology systems that would need to be connected, and implementation could occur in-house. Thus, these data providers would be able to move more quickly to implement the proposed rule's requirements."[14]

TYPES OF DATA COVERED

A data provider must make available to a consumer and the consumer's "authorized third party" upon request "covered data" that it has in its control or possession at the time of the request.[15]An authorized third party means a third party that has complied with the authorization procedures specified in the Open Banking Rule.[16]The data made available must be the most recently updated data that it has at the time of the request, including "authorized but not yet settled debit card transactions."[17] Although the proposed rule requires that access be provided to the most recently updated data, the CFPB explains that the requirement is not intended to limit a consumer's right to access historical covered data.[18]

"Covered data"[19]that must be made accessible includes six categories of data and four exceptions:

Required Data Types

1. Transaction data including at least 24 months of historical data in the control or possession of the data provider. Transaction data includes:
   - amount,
   - date,
   - payment type,

- pending or authorized status,
- payee or merchant name,
- rewards,
- credits, and
- fees or finance charges.

2. Account balance.
3. Information to initiate payment to or from a Reg E Account, such as routing and account numbers to initiate an ACH transaction. The data provider may provide a tokenized account and routing number in addition to, or instead of, a non-tokenized account and routing number (note - the CFPB's discussion of tokens does not consider whether the consumer's and authorized third party's payees would be required to revert to the data provider to use the tokenized information, i. e., would a consumer's successor bank or fintech still be tethered to the issuer of the token?).[20]
4. Terms and conditions, including as applicable, (at least):
   - the applicable fee schedule,
   - any annual percentage rate or annual percentage yield,
   - rewards program terms,
   - whether a consumer has opted into overdraft coverage, and
   - whether a consumer has entered into an arbitration agreement.
5. Upcoming bill information including bill payments due to the provider and scheduled payment to third party billers, e. g., through the data provider's bill payment service.
6. Account verification information associated with the specific product or service, limited to:
   - name
   - address
   - email address
   - phone number

Note: Social Security Numbers are not required to be made accessible.[21]

Exceptions[22]

Data providers are not required to provide access to:

1. "Confidential commercial information," for example, an algorithm used to generate risk predictions, etc., although the data derived from such algorithms is not excepted if it is otherwise required to be provided.

2. Information gathered solely for the purpose of prevention of fraud or money laundering or monitoring for unlawful conduct, but not identity information otherwise required to be made available.

3. Information required to be kept confidential from the consumer, but the provider may not withhold data merely because it is subject to data privacy protections.

4. Any information that the data provider cannot retrieve in the ordinary course of business.

Note: The CFPB does not intend the 4th exception to be used to circumvent the specific data accessibility requirements, and admonishes generally that "The CFPB intends to monitor the market for pretextual use of the CFPA section 1033 exceptions."[23]

REQUIRED ACCESS INTERFACES

Covered data providers are required to provide a "consumer interface" and a "developer interface." This wording appears to refer to what is commonly called an "application programming interface" or "API" but may have a different technical scope. It is not clear why the CFPB chose to use different terminology, although it may arise from the functionality limited to data retrieval that is required to be supported by the consumer and developer interfaces as prescribed by the proposed rule (as discussed above).

CONSUMER INTERFACE

Data providers must provide a consumer interface and a developer interface, each of which must satisfy certain requirements.[24]Covered data must be made available to the consumer and the consumer's authorized third party in "a machine readable file that can be retained by the consumer or authorized third party and transferred for processing into a separate information system that is reasonably available to and in the control of the consumer or authorized third party."[25]The data provider may not charge for establishing and maintaining the required interfaces or for receiving and responding to a request for access to covered data.[26]The data provider may charge fees through the consumer interface for other services that are charged irrespective of whether the

consumer uses the interface, such as for payment services, account maintenance fees or other account services.[27]

DEVELOPER INTERFACE

The CFPB provides more elaborately for the "developer interface" that data providers must make available. The purpose of the developer interface is to provide for access to data for qualified third party service providers designated by consumers to have access to their individual data without having to rely on screen scraping practices. The CFPB views screen scraping, which requires the consumer to disclose their website access credentials to the third party, as presenting "risks to consumers and the market … and complicat[ing] the mechanics of data access, particularly with respect to authentication and authorization procedures for data providers." In addition to the risks arising from disclosure of consumers' access credentials, the CFPB cited risks of overcollection of data, inaccuracy of data and compromise of consumer privacy. Therefore, the proposed Open Banking Rule does not require that data providers permit screen scraping.[28]

STANDARDIZED DATA FORMAT

The format for data, i.e., the order and content of data fields, status codes and communication protocols, of the machine readable data set, must be "standardized," The CFPB's stated goal of requiring a standardized format is "to ensure that the information systems of, in particular, new-entrant and small-entity third parties can process covered data from the full range of data providers across the market by reducing the extent of varied and idiosyncratic formats that impel reliance on intermediaries to provide data in a usable format."[29]The proposal does not prescribe a specific standard data format. Instead, the proposal requires the data provider to use a "qualified industry standard" or if none is available, a format that is "widely used by the developer interfaces of other similarly situated data providers with respect to similar data and is readily usable by authorized third parties."[30]A qualified industry standard is defined as

> "a standard issued by a standard-setting body that is fair, open, and inclusive …"[31]

A fair, open and inclusive standard-setting body has the following attributes:

i. openness to all interested parties;

ii. balance across all interest groups at all levels of the standard-setting body;

iii. provides due process including notices, opportunity to express views and a fair process for resolving conflicting views;

iv. provides an appeals process for resolving conflicting views;

v. proceeds by consensus, though not necessarily unanimity;

vi. provides transparency to participants and to the public; and

vii. has been recognized (recently) by the CFPB as an issuer of qualified industry standards.[32]

The CFPB has not determined whether such qualified industry standards exist and requests comments on whether implementation deadlines should be extended to facilitate development of qualified industry standards.[33]The absence of such a standard or such a CFPB-recognized standard setting body would leave data providers, consumers and authorized third parties to rely on the aforementioned "widely used by the developer interfaces of other similarly situated data providers with respect to similar data …."[34]

PERFORMANCE SPECIFICATIONS

Where the proposed rule prescribes a specific standard, the CFPB proposes that a data provider must provide "proper responses" to at least 99.5% of queries for covered data within not more than 3,500 milliseconds (i.e., 3.5 seconds).[35]The CFPB points out that data providers mostly already meet or exceed this standard and that this standard is aligned with response times required in Australia and the UK.[36] Otherwise, the developer interface is required to perform in a "commercially reasonable" manner, with allowances for "reasonable" scheduled downtime."[37]Further data providers are prohibited from "unreasonably" restricting the frequency or number of requests for covered data from an authorized third party and must document the restrictions in the data provider's written policies and procedures.[38]

SECURITY SPECIFICATIONS

The data provider may not permit access to its developer interface by using credentials that a consumer uses to access its consumer interface.[39]The CFPB explains that this prohibition is intended to curtail screen scraping.[40]In addition to this specific prohibition, the proposed rule would require data providers that are financial institutions covered by the Gramm-Leach-Bliley Act[41]to apply a data security program to their developer interface that satisfies the GLBA Safeguards Framework. If the covered data provider is not subject to the GLBA, the data provider must comply with the Federal Trade Commission's Standards for Safeguarding Customer Information.[42]The CFPB cites security obligations of financial institutions to secure their own operations and to establish practices to manage risks arising from third party relationships.[43]

INTERFACE ACCESS AND RESPONSES TO REQUESTS FOR INFORMATION

The proposed rule provides for a data provider to deny access to a consumer's information through an interface under reasonable circumstances, including for risk management purposes that are applied in a consistent, non-discriminatory manner.[44]The CFPB explains that as used in this

context, the term "non-discriminatory" "carries its ordinary meaning and is not intended to refer to discrimination on a prohibited basis under Federal fair lending law."[45]The proposed rule prescribes conditions for providing information in response to a consumer or third party request, such as consumer and third party identity authentication, and exceptions to the requirements for responses.[46]The CFPB discusses these authentication conditions in detail and further explains that data providers may not use authentication and other procedures based on subjective risk management concerns to deny responses to requests for information in most circumstances because such generalized concerns often involve the exercise of discretion by data providers, which might undermine the objectives of the rule to allow consumers' designated third parties access to data so as to promote competition with the data provider.[47] However, the CFPB proposes that a data provider would have a reasonable basis for denying a third party access to a developer interface if a third party does not present evidence that its security practices are "adequate."[48]A data provider may provide consumers a reasonable method for revoking a third party's access to the consumer's covered data.[49]The CFPB requests comments on whether data providers should be required to notify the CFPB of all third parties that they have granted access to their developers interface and to notify the CFPB when they deny access to a third party, noting also that such information would be made public.[50]

DATA PROVIDERS' PUBLIC DISCLOSURES; POLICIES AND PROCEDURES

REQUIRED DISCLOSURES

Covered data providers must publicly disclose certain information in both human and machine readable form, including identifying information, their Legal Entity Identifier, website link and contact information to be used by consumers to get information about accessing covered data.[51]The data provider must also make available developer interface documentation sufficient for a third party to access and use the developer interface, including "metadata describing all covered data and their corresponding data fields …"[52]Finally, a covered data provider must disclose on or before the 10th day of each calendar month, the quantitative minimum performance achieved by its developer interface during the previous calendar month, for a rolling 13-month period, described as a percentage rounded to four decimal places (e. g., 99.9999 percent).[53]

POLICIES AND PROCEDURES; RECORD KEEPING

A covered data provider must establish and update written policies for compliance with the Open Banking Rule. The policies must cover procedures for making covered data available, records of denials of access to developer interface, records of denials of specific information requests, ensuring accuracy of data transmissions (but not accuracy of the underlying data on the data provider's records), and record retention. Records relating to responses to consumers' and third

party's requests for information or access to the developer's interface must be kept for 3 years and other records of compliance must be kept for "a reasonable period."[54]

AUTHORIZED THIRD PARTIES

CONSUMER AUTHORIZATION OF THIRD PARTY

To be designated an "authorized third party," an organization must obtain the consumer's express informed consent to access covered data by obtaining an authorization disclosure in the prescribed format that is signed by the consumer, either electronically or in writing. The third party must provide the consumer a statement certifying that it agrees to certain prescribed obligations.[55]The disclosure must be clear, conspicuous, and separate from other material. The required disclosure must include certain specified data elements regarding the identity of the third party, the services to be provided using the consumer's data that will be accessed, the types of data that will be accessed, and the revocation mechanism.[56]The CFPB determined that the Americans with Disabilities Act and implementing regulations would independently require that the authorization disclosure be provided in an accessible format.[57]

THIRD PARTY OBLIGATIONS.

In obtaining the consumer's consent to access data, the third party must agree in writing to meet certain prescribed obligations.

1. **Data collection.** The third party must agree that:

   - Collection, use and retention of data will be limited to data that is reasonably necessary to provide the consumer's requested service or product,
   - Accessed covered data will not be used for targeted advertising, cross-selling of other products or services, or be sold to further third parties,
   - Access to data will be limited to one year after the consumer's consent,
   - The third party may request consent to access the consumer's data for an additional one-year term, and
   - If a further consent is not obtained, the third party will cease data collection and will not retain data previously collected.[58]

2. **Data uses.** Data may be used and disclosed to additional third parties to use accessed data:

   - To comply with law or legal process,

- As reasonably necessary to prevent fraud and unauthorized transactions, and
- In servicing or processing the product or service that the consumer requested, subject to the same restrictions that apply to the authorized third party.[59]

3. **Accuracy of data**. The third party must develop and periodically review policies and procedures for insuring accuracy in its receipt and transmission of the consumer's data.
4. **Data security.** As noted above, an authorized third party must comply with, as applicable, the data security provisions of Section 501 of the Gramm-Leach-Bliley Act or the requirements of the Federal Trade Commission's Standards for Safeguarding Customer Information.[60]
5. **Further disclosure.** An authorized third party that discloses covered data to further third parties for permitted purposes must obtain the receiving third party's agreement to comply with the same obligations that apply to the authorized third party.[61]
6. **Record Retention.** An authorized third party must establish written policies and procedures for retention of records demonstrating compliance. Such records must be retained for not less than 3 years after a consumer's most recent authorization. Records must include (i) copies of each consumer's authorization disclosure that shows the date of the consumer's signature or electronic consent and of any actions of revocation of consent taken by the consumer; and (ii) if a data aggregator is used to facilitate access to covered data, copies of the separate authorization disclosure provided to consumer by or on behalf of the data aggregator.[62]

USE OF DATA AGGREGATORS

A "data aggregator" is defined as a third party engaged by an authorized third party to enable its access to covered data.[63]The authorized third party remains responsible for both the data aggregator's and its own compliance with the consumer authorization procedures that apply to the authorized third party. The authorization disclosure provided to the consumer must include the name of any data aggregator that will assist the third party seeking the consumer's authorization and describe the services to be provided by the data aggregator. Before accessing a consumer's covered data, the data aggregator must certify to the consumer its agreement to comply with the conditions on access and usage that are required of the authorized third party.[64]

FOOTNOTES

[1] https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-jumpstart-competition-and-accelerate-shift-to-open-banking/

[2] Consumer Protection Financial Protection Act of 2010, Title X, §1033; Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. 111-203, 124 Stat. 1376, 2008 (2010). The Open Banking Rule would add Part 1033 to 12 CFR Title X.

[3] Notice or Proposed Rulemaking, https://files.consumerfinance.gov/f/documents/cfpb-1033-nprm-fr-notice_2023-10.pdf 88 FR 75796 (October 31, 2023)

[4] See CFPB's discussion of marketplace mechanisms that would encourage migration to usage of the mandated API access. Notice of Proposed Rulemaking, p. 19.

[5] 12 U.S.C. 5533(a), 124 Stat.2008, P.L. 111-203, (July 21, 2010).

[6] 12 CFR §1033.1111(a). (Citations are to sections of the proposed regulation as enumerated in the Notice of Proposed Rulemaking.) https://files.consumerfinance.gov/f/documents/cfpb-1033-nprm-reg-text-with-1001_2023-10.pdf

[7] 12 CFR §1033.1111(b).

[8] Notice of Proposed Rulemaking, p. 31.

[9] 12 CFR §1033.1111(c).

[10] 12 CFR §1033.1111(d).

[11] 12 CFR §1033.131.

[12] Notice of Proposed Rulemaking, p.43.

[13] Notice of Proposed Rulemaking, p.40-41 (footnotes omitted).

[14] Notice of Proposed Rulemaking, p.41 (footnotes omitted).

[15] §1033.201(a).

[16] The authorization procedures are prescribed in §1033.401.

[17] §1033.201(b).

[18] Notice of Proposed Rulemaking, p. 54.

[19] §1033.211.

[20] See Notice of Proposed Rulemaking, p. 60.

[21] Notice of Proposed Rulemaking, p. 63.

[22] §1033.221.

[23] Notice of Proposed Rulemaking, p. 66.

[24] §1033.301(a).

[25] §1033.301(b).

[26] §1033.301(c)

[27] Notice of Proposed Rulemaking, p. 72.

[28] Notice of Proposed Rulemaking, pp. 68-69.

[29] Notice of Proposed Rulemaking, p. 75.

[30] §1033.311(b)

[31] §1033.131

[32] §1033.141(a)

[33] *Id.* at p. 76.

[34] §1033.311(b).

[35] §1033.311(c)(1)(d)(3).

[36] Notice of Proposed Rulemaking, pp 79-80.

[37] §1033.311(c)(1).

[38] §1033.311(c)(2).

[39] §1033.311(d)(1).

[40] Notice of Proposed Rulemaking, p. 85.

[41] 15 U.S.C. 6801 *et seq*.

[42] §1033.311(d)(2). See 16 CFR part 314.

[43] Notice of Proposed Rulemaking, p. 92, fns 86-87.

[44] §1033.321.

[45] Notice of Proposed Rulemaking, p. 92.

[46] §1033.331.

[47] Notice of Proposed Rulemaking, p. 95.

[48] Notice of Proposed Rulemaking, p. 96.

[49] §1033.331(e).

[50] Notice of Proposed Rulemaking, pp. 100-101.

[51] §1033.341(a)-(b).

[52] §1033.341(c).

[53] §1033.341(d).

[54] §1033.351(a)-(d).

[55] §1033.401.

[56] §1033.411.

[57] Notice of Proposed Rulemaking, p. 134, *citing* 42 U.S.C. 12132, 12182(a); 28 CFR 35.130, 35.160(a), 36.201, 36.303(c).

[58] §1033.421

[59] §1033.421(c).

[60]§1033.421(e).

[61] §1033.421(f).

[62] §1033.441.

[63] §1033.131.

[64] §1033.431.

RELATED PRACTICE AREAS

- Finance
- Fintech
- Banking Sector
- Data Privacy & Security

MEET THE TEAM

Stanton R. Koppel

San Francisco

stanton.koppel@bclplaw.com
+1 415 675 3437
