CFPB's Outline of Proposals to Implement Dodd-Frank § 1033

December 1, 2022

On October 27, 2022, the Consumer Financial Protection Bureau (the "CFPB") issued an outline of proposals and alternatives under consideration (the "Outline")[1] for its rulemaking to implement section 1033 of the Dodd–Frank Wall Street Reform and Consumer Protection Act, 12 U.S.C. § 5533 ("Section 1033"). Section 1033 requires covered persons within the meaning of the Consumer Financial Protection Act of 2010 ("CFPA")[2] to provide to consumers upon request information in the covered person's control or possession concerning the consumer's financial product or service with the covered person.[3] Under the Small Business Regulatory Enforcement Fairness Act of 1996 ("SBREFA"), the CFPB is required to convene a small business review panel to collect advice and recommendations from small entity representatives.[4] The Outline is intended to facilitate that process by providing an overview of the proposals being considered by the CFPB.

The Outline is the latest in the CFPB's steps toward promulgating a rule to implement Section 1033, following its February 2020 symposium with industry stakeholders and its November 2020 Advance Notice of Proposed Rulemaking ("ANPR").[5] The CFPB will still need to promulgate a proposed rule, go through a formal comment period and put forward a final rule. The Outline provides insight on the CFPB's development of the rule and is thus a valuable tool to the broader market of providers of consumer financial products and services.

---

1 Outline of Proposals and Alternatives Under Consideration, October 27, 2022, *available* at https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf.

2 The CFPA defines "covered persons" as "(A) any person that engages in offering or providing a consumer financial product or service; and (B) any affiliate of a person described in subparagraph (A) if such affiliate acts as a service provider to such person." 12 U.S.C. § 5481(6).

3 In addition, under Section 1033, the CFPB must prescribe standards applicable to covered persons to promote the development and use of standardized formats for information to be made available to consumers. *See* 12 U.S.C. § 5533(d); Outline p.3.

4 The CFPB expects that outside of the financial industry, affected entities will include software publishers, data hosting services, payroll services and credit bureaus (among others). Outline p. 52.

5 *See* our previous discussion of the ANPR here.

The Outline is divided into seven sections, which can be organized into two general categories: (i) substantive requirements including who is subject to the rule, to whom they must provide information and what information they must provide; and (ii) procedural requirements including how information should be made available, third-party obligations and record retention guidelines.[6] Here, we focus on both the substantive and procedural requirements while providing commentary on the impact of the proposals from an industry perspective.

Substantive Requirements

Who Is Covered by the Rule?

At the outset, the CFPB is considering limiting those subject to the rule to entities that meet either the definition of "financial institution" under Regulation E[7] or "card issuer" under Regulation Z[8] (collectively, "Covered Data Providers"). The Outline indicates that the CFPB intends to prescribe rulemaking that will subject other covered persons to Section 1033 in the future (*e.g.*, government benefit accounts, other providers of credit products). Specifically, under the CFPB's current proposal:

- ***Financial institutions*** would include banks, credit unions and other persons that directly or indirectly hold an account of a consumer and persons that issue an access device and agree with a consumer to provide electronic fund transfer ("EFT") services. The financial institution would only be a Covered Data Provider with regard to qualifying accounts and access devices it issues.

- ***Card issuers*** would include persons that issue credit cards and their agents with respect to the card. A card issuer would only be a Covered Data Provider with respect to a "credit card account under an open-end (not home-secured) consumer credit plan"; however, a card issuer that does not hold consumer credit card accounts but that issues credit cards would be a Covered Data Provider with respect to the consumer credit card transactions it processes.

The CFPB may consider exemptions to the rule for certain financial institutions or card issuers, based on factors such as asset size and/or the number of accounts, but the Outline does not provide any specific proposals in this regard.

---

6 The seven sections in the Outline are: (i) coverage of data providers who would be subject to the proposals; (ii) recipients of information; (iii) types of information covered; (iv) how/when information would need to be made available; (v) third-party obligations; (vi) record retention guidelines; and (vii) implementation period.

7 12 CFR 1005.2(i).

8 12 CFR 1026.2(a)(7).

Commentary:

- Smaller financial institutions or those less active in the consumer product space should consider whether to advocate during the formal rulemaking process for exemptions from the eventual proposed rule.

- However, entities not subject to the current rulemaking should nevertheless remain attuned to the requirements because the CFPB has indicated an interest in eventually expanding the scope of covered persons subject to the rule.

To Whom Must Information Be Made Available?

Section 1033 requires that Covered Data Providers make information available to consumers including individuals and agents, trustees or representatives acting on behalf of an individual consumer (referred to as "third parties").[9] However, a Covered Data Provider is only required to make the information available if it believes the party has authorization.

Evidence Reflecting Consumer Authorization

The CFPB is considering proposing that a Covered Data Provider be required to make information available to a consumer if it can reasonably authenticate the consumer's identity and reasonably identify the information requested.

Evidence Reflecting Third Parties' Authorization

To protect against fraudulent attempts by third parties to access consumer data, the CFPB is considering proposing that a Covered Data Provider would only need to make information available, upon request, when it receives (i) information sufficient to authenticate the identity of the third party, (ii) evidence of consumer authorization (discussed directly below) and (iii) information identifying the scope of information requested.

The CFPB expects to set specific standards through which a Covered Data Provider can determine which third parties are authorized to act on behalf of a consumer. The Outline lays out three components of sufficient third-party authorization: (1) an "authorization disclosure" provided by a third party to the consumer; (2) the consumer's informed, express consent to the key terms of access contained in the disclosure; and (3) a certification statement.

Authorization Disclosure. The authorization disclosure would need to disclose the general categories of information to be accessed, the name of the Covered Data Provider and accounts to be accessed, the duration and frequency of access, and how the user can

---

[9] The Outline does not address how requests for information should be treated when accounts are owned by multiple consumers, including when only one of the consumers requests information.

revoke access. The disclosure would also need to describe the terms of use of the information, such as the intended recipients of the information (including any downstream parties) and the purpose for accessing the information. In terms of timing, the CFPB is considering requiring the disclosure to be provided close in time to when the information is requested (seemingly eliminating the possibility of satisfying this standard with an advance, blanket authorization).

Consumer Consent. The third party would be required to obtain consent from the consumer in written or electronic form, evidenced by the consumer's signature or electronic equivalent and may also be required to mail or electronically send a copy of the signed consent to the consumer.

Certification Statement. The third party would need to certify that it will abide by certain obligations regarding use, collection and retention of the consumer's information. (See Third-Party Obligations section below).

Commentary:

- The disclosure and consent pieces of the authorization process could help ensure consumer authorization is informed and explicit.

- Market participants may wish to consider whether any of the authorization requirements are extraneous or overly burdensome. For example, the certification statement may be redundant, as the Outline elsewhere recommends having collection, use and retention rules. Requiring disclosure close in time to when the information would be needed may also be burdensome for time-sensitive disclosures when consumers may be slow to consent.

Types of Information Covered

Information Categories. There are five enumerated categories of information the CFPB is considering requiring Covered Data Providers to make available with respect to covered accounts:

- Periodic statement information for settled transactions and deposits of the type that is generally required to be provided under Regulation Z, Regulation DD and Regulation E;

- Information regarding prior transactions and deposits that have not yet settled;

- Other information about prior transactions not typically shown on periodic statements or portals;[10]

- Online banking transactions that the consumer has set up but that have not yet occurred; and

- Account identity information (*e.g.*, name, age, social security number).

The CFPB is also considering requiring Covered Data Providers to make available:

- consumer reports from consumer reporting agencies, such as credit bureaus, obtained and used by the Covered Data Provider in deciding whether to provide an account or other financial product or service to a consumer;

- fees that the Covered Data Provider assesses in connection with its covered accounts;

- bonuses, rewards, discounts, or other incentives that the Covered Data Provider issues to consumers; and

- information about security breaches that exposes a consumer's identity or financial information.

The CFPB is considering requiring a Covered Data Provider to make available the most current information they have in their control or possession as well as information going as far back in time as such Covered Data Provider makes transaction history directly available to consumers.

Exceptions. The Outline also discusses the four categories of information that are expressly excluded from Section 1033's coverage:

- Confidential commercial information, including algorithms and inferences derived about consumers, their credit scores and other predictors from Covered Data Providers' proprietary models;

- Any information collected by the Covered Data Provider for the purpose of preventing fraud or money laundering, or detecting or making any report regarding other unlawful or potentially unlawful conduct. The Outline indicates that the CFPB is considering interpreting "for the purpose of" to mean information that a Covered Data Provider actually uses to prevent fraud or money laundering, or to detect or

[10] Information about prior transactions not typically shown on periodic statements or portals typically includes data elements obtained from payment networks about each payment transaction.

report potentially unlawful conduct, or that the Covered Data Provider would not have collected but for a legal requirement to collect the information for these purposes;

- Any information required to be kept confidential by any other provision of law. The Outline indicates that the CFPB is considering interpreting this category to mean information subject to a statutory or regulatory requirement to keep the information confidential from the consumer; and

- Any information that the Covered Data Provider cannot retrieve in the ordinary course of its business.

The Outline also includes general questions regarding all four enumerated exceptions in Section 1033. For example, the CFPB is considering whether it should require Covered Data Providers to disclose to consumers or authorized third parties the reason information is not available pursuant to the four enumerated exceptions. Accordingly, further insight regarding each of the exceptions may be expected in an eventual proposed rule.

Commentary:

- The framework in the Outline for the scope of data covered appears to attempt to balance company and consumer interests.

- Online banking transactions that the consumer has set up but that have not yet occurred, as well as information regarding prior transactions and deposits that have not yet settled, may be beneficial to consumers in managing their finances, identifying potentially erroneous transactions and preventing overdrafts—including with respect to APSN (authorize positive, settle negative) transactions. These data elements may also be very challenging for financial institutions to generate and provide.

- The CFPB has not yet defined the exceptions about providing "confidential commercial information" and information the institution "cannot retrieve in the ordinary course of its business." Given the potential ambiguity of these terms, it may be useful for companies to comment on their scope.

Procedural Requirements

How Information Would Be Made Available

For consumers, the CFPB is considering proposing that all Covered Data Providers make information available through online financial account management portals and allow consumers to export the information covered by the proposals in both human and machine-readable formats.[11]

For third parties, the CFPB is considering proposing that Covered Data Providers establish and maintain a third-party portal that does not require the authorized third party to possess or retain consumer credentials. This is in line with market trends and would mark a step away from screen scraping,[12] which, according to the Outline, "presents some significant limitations and risks to consumers, data providers, and third parties, including risks related to possession of a consumer's credentials."

The CFPB may impose specific requirements on these portals regarding: (i) availability of information, (ii) accuracy of the information and (iii) security. For example, the CFPB is considering requirements relating to portal uptime, latency, unplanned outages, error response and access caps.

See the Third-Party Obligations section below for a discussion of accuracy and data security and the To Whom Must Information Be Made Available? section above for a discussion of third-party authorization requirements.

Commentary:

- For larger existing data providers, these requirements may not be costly or difficult to develop, but small businesses and new companies may have difficulty building out these capabilities.

- While commercial and legal pressures have reduced the prevalence of screen scraping, it is still a common method for information sharing. If the CFPB requires third parties to access data through a separate portal, then this could represent a significant compliance burden for parties relying on screen scraping and a boon to those who have already abandoned screen scraping and moved on to other technology.

---

[11] *See* 12 U.S.C. § 5533(a); (d).

[12] "Screen scraping" means a third party's use of proprietary software to convert consumer data presented in the provider's online financial account management system—typically through the use of the consumer's credentials—into standardized machine readable data, generally on an automated basis. Outline p. 68.

- In the Outline, the CFPB poses questions about industry standards for the portal, particularly regarding application programming interfaces, indicating that further comments on this point may be useful to advocate for specific solutions.

Third-Party Obligations

The CFPB expects to prohibit third parties from collecting, using or retaining information beyond what is reasonably necessary to provide the product or service requested by the underlying consumer. The CFPB also expects third parties to be bound by data security and accuracy obligations.

- ***Collection***. With regard to collection, the Outline suggests that the CFPB may set limits on the duration and frequency of access to information and require the third-party to provide consumers with periodic reminders of their ability to revoke authorization or a simple way for the consumer to revoke access. In line with their proposed reasonable policy standard for Covered Data Providers, the CFPB plans to propose a maximum period of access after which the third party would need to renew its authorization.

- ***Use***. With regard to use, the CFPB is considering distinguishing between primary use (information that is reasonably necessary to provide the product or service) and secondary use (information beyond what is reasonably necessary, including the third party's own use of consumer data and the sharing of data with downstream entities). The Outline presents four potential approaches to secondary uses:

  - Prohibiting secondary uses completely;

  - Prohibiting "high risk" secondary uses;

  - Requiring the consumer to opt in to secondary uses; or

  - Permitting secondary use unless the consumer opts out.

- ***Retention***. The CFPB is considering requiring third parties to retain consumer information only until information is no longer reasonably necessary to provide the product or service or upon revocation of the third-party authorization. The CFPB expects a proposed rule to provide an exception for any information required to be retained to comply with other laws.

- ***Data Security***. The Outline also discusses potential data security and data accuracy standards for third parties, but notes that both may already be sufficiently covered by other privacy and data protection regimes. With regard to data security, the Gramm-

Leach-Bliley Act ("GLBA") likely already applies to most Covered Data Providers, so the CFPB may:

- leave the rules as they are;
- require third parties to develop, implement, and maintain a comprehensive and tailored written data security program; or
- require compliance with GLBA standards framework implemented by the FTC or prudential regulators.

- ***Data Accuracy.*** The CFPB is considering requiring third parties to maintain reasonable policies and procedures to ensure data accuracy, including dispute procedures. While the CFPB acknowledges this is covered by some other regulatory regimes,[13] it also notes that there are still no general accuracy requirements for data collection.

Commentary:

- A duration requirement might help consumers keep track of their data permissions and avoid unintentional lingering authorities.
- Some of the proposals regarding third-party access appear to be aimed at providing consumer privacy protections at a relatively low cost.
- The data protection and security procedures proposed by the Outline may prove difficult for smaller players such as fintech companies.
- The CFPB has asked for comment on how to define "high risk" secondary uses, which may be a salient topic for comment from entities whose business is predicated in whole or in part on the insights derived from consumer data.

Record Retention Guidelines

The CFPB is considering proposing record retention requirements for Covered Data Providers and third parties to demonstrate compliance with the rule but does not provide any specifics at this stage. The requirements would apply only to information that would need to be disclosed to a consumer under Section 1033.

---

[13] Per the Outline, "FCRA and Regulation V impose accuracy requirements on the information furnished to and provided by consumer reporting agencies, EFTA and Regulation E protect consumers against unauthorized electronic fund transfers and other errors, and TILA and Regulation Z, and RESPA and Regulation X protect consumers against certain billing and servicing errors." Outline p. 46.

Conclusion

While the Outline was developed primarily to fulfill the CFPB's obligations under the SBREFA, it is the latest indication that the CFPB remains interested in ensuring consumers' financial data access rights under Section 1033. While there is no formal comment period at this stage in the rulemaking, all entities—including those that are not small businesses—should provide comments by January 25, 2023, which is 90 days after the Outline's publication.

The requirements under consideration by the CFPB appear to represent thoughtful attempts at ensuring consumers have better knowledge of and control over their data. However, there are areas where the information potentially covered by the rule and the related procedures could prove costly and burdensome for Covered Data Providers and third parties.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Courtney M. Dankworth
cmdankworth@debevoise.com

Avi Gesser
agesser@debevoise.com

WASHINGTON, D.C.

Jehan A. Patterson
jpatterson@debevoise.com

NEW YORK

Anna R. Gressel
argressel@debevoise.com

Alexandra N. Mogul
anmogul@debevoise.com

Jonathan Steinberg
jrsteinberg@debevoise.com

Catherine Morrison
ccmorrison@debevoise.com