November 9, 2023

Proposed CFPB Rule on Personal Financial Data Rights

Proposal Would Accelerate Shift Toward "Open Banking" by Granting Consumers Rights of Access and Portability for Payment Account-Related Data and Establishing Requirements for Data Sharing

SUMMARY

On October 19, 2023, the Consumer Financial Protection Bureau released a proposed rule[1] that marks the CFPB's first rulemaking under section 1033 of the Consumer Financial Protection Act of 2010 (the "CFPA").[2] Section 1033 generally empowers the CFPB to prescribe rules under which providers of consumer financial products or services must make data available to their consumers regarding the products or services consumers obtain.

Although section 1033 may be applied to a wide range of consumer financial products and services, the proposed rule focuses on data related to payments and payment accounts. Banks, credit unions, and other providers of checking, savings, and credit card accounts and various other payments accounts and products, including digital wallets, would have to make a broad range of information available to consumers through "consumer interfaces" and to consumer-authorized third parties through "developer interfaces." These third parties, which would include financial technology companies (fintechs), data aggregators collecting data for fintechs, banks, and others, would access the information in connection with providing the consumer with other financial products or services. The proposed rule would impose a number of obligations with respect to both the provision of data through consumer and developer interfaces and third party access to that data. The proposed rule would be implemented in phases, with the largest providers being subject to its requirements within approximately six months after a final rule is published and smaller banks and credit unions having several years before compliance becomes required.

According to the CFPB, the proposed rule would "accelerate a shift toward open banking, where consumers would have control over data about their financial lives and would gain new protections against companies misusing their data."[3] It would also "jumpstart competition" by permitting consumers to direct existing providers to "share data . . . with other companies offering better products" and enabling consumers "to walk away from bad service."[4] The proposed rule would prohibit third parties that receive covered data from collecting, using, or retaining the data "to advance their own commercial interests," including through targeted advertisements, and would "seek[] to move the market away" from "screen scraping."[5]

Comments on the proposed rule are due by December 29, 2023. CFPB Director Rohit Chopra said in a statement that the CFPB will seek to finalize a rule by fall of 2024.[6]

I. BACKGROUND

Section 1033 of the CFPA was enacted in 2010, as part of the Dodd-Frank Wall Street Reform and Consumer Protection Act, with a view to ensuring that consumers would have largely unfettered access to, and control over, their financial data. The provision applies to "covered persons," a term defined broadly in the CFPA to include "any person that engages in offering or providing a consumer financial product or service" and affiliate service-providers of such persons.[7] Under section 1033, subject to rules to be promulgated by the CFPB, a covered person must make available to consumers information in the covered person's possession or control concerning the consumer financial product or service obtained by the consumer, subject to four exceptions.[8] Section 1033 also directs the CFPB to prescribe, by rule, standards "to promote the development and use of standardized formats for information, including through the use of machine readable files," for the information to be made available to consumers under the provision.[9]

Over the next decade, the CFPB sought to understand and shape marketplace developments related to sharing of personal financial data, but did not take action to promulgate the rules required by section 1033. In 2016, the CFPB published a request for information, seeking public comment so that it could "better understand the consumer benefits and risks associated with market developments that rely on access to consumer financial account and account-related information."[10] The following year, the CFPB released a set of "Consumer Protection Principles" that addressed consumer-authorized access to account data and related consumer protection challenges, particularly in respect of data privacy and security.[11]

In 2020, the CFPB took more concrete steps toward the rulemaking contemplated by section 1033. It held a symposium to "hear from stakeholders and to review the [CFPB's] approach to consumer-authorized third-party access to financial records."[12] It also issued an Advanced Notice of Proposed Rulemaking ("ANPR") to solicit comments to assist the CFPB in developing rules to implement section 1033.[13] One hundred comments were received on the ANPR.[14]

The movement toward a proposed rule under section 1033 accelerated in the Biden Administration. In July 2021, within months of being sworn into office, President Biden, as part of an executive order aimed at

promoting competition, "encouraged" the CFPB to consider "commencing or continuing a rulemaking under section 1033 . . . to facilitate the portability of consumer financial transaction data so consumers can more easily switch financial institutions and use new, innovative financial products."[15] Around that same time, Rohit Chopra, who at the time was President Biden's nominee for CFPB Director, voiced a commitment to moving the rulemaking on section 1033 forward.[16]

In October 2022, the CFPB published an outline of proposals and alternatives it was considering in implementing section 1033.[17] This outline was in furtherance of procedural requirements that require the CFPB to convene a small business review panel with respect to any rulemaking expected to have a significant economic impact on a substantial number of small entities.[18] The required review panel was held in February 2023, with a final report published the following month.[19] The CFPB also published in early 2023 two sets of market monitoring orders to collect information from data aggregators and large data providers related to the CFPB's section 1033 rulemaking efforts.[20] Both Director Chopra and senior Treasury Officials have recently emphasized the importance of the rulemaking.[21]

The proposed rule reflects the culmination of these multi-year efforts.[22]

II. OVERVIEW OF THE PROPOSED RULE

A. Summary

The proposed rule focuses on data related to payments and payment accounts and would require "data providers"—including almost all banks and credit unions and all providers of various other payment accounts and products, including digital wallets—to make available a broad range of information. This information would include details of individual transactions, account balances, routing and account numbers, terms and conditions, upcoming bill information, and basic account verification details. The required information would need to be made available *both* directly to a consumer through a "consumer interface" (such as online banking or a mobile app) *and* to "third parties" through a "developer interface" (also known as an application programming interface or API). A third party, including a data aggregator collecting data for another third party, would require express consumer authorization to access this data through a developer interface and would be required to limit its collection, use, and retention of covered data to what would be reasonably necessary to provide the consumer with a requested product or service. The CFPB gives, as examples of the third party products that may rely on covered data, personal financial management tools, payment applications and digital wallets, credit underwriting (including cashflow underwriting), and identity verification.[23]

The proposed rule would impose a number of requirements on data providers with respect to their consumer and developer interfaces and on third parties with respect to accessing covered data. Developer interfaces would need to provide the information in a standardized format, satisfy commercially reasonable performance standards, and meet security standards. Data providers would also need to publish

information regarding their developer interfaces and implement written policies and procedures addressing data availability, data accuracy, and record retention. In obtaining express consumer authorization to access data, third parties would need to, among other things, provide clear, segregated disclosures to consumers and certify their compliance with various obligations, including the requirement noted above that third parties limit their collection, use, and retention of covered data to what is reasonably necessary to provide a requested product or service. Third parties would also be required to seek consumer reauthorization at least annually to continue collecting data, comply with data accuracy and data security requirements, enable and effect consumer requests to revoke access to information, and require downstream recipients of covered data to agree, with limited exceptions, to the same obligations. Third parties would additionally need to implement written policies and procedures. Third parties that engage a data aggregator to access data would be responsible for the data aggregator's compliance with the rule, and the data aggregator would also be subject to specific obligations.

Furthermore, under the proposed rule, only in limited circumstances could a data provider refuse a consumer's or authorized third party's access to covered data, and a data provider could not charge a fee for access or impose an unreasonable restriction (such as an access cap or rate limit) on the frequency of access. The permitted circumstances for refusing access would include: when covered data is subject to an exemption in section 1033 (*e.g.*, confidential commercial information, including an algorithm used to derive credit or other risk scores); when the data provider has reasonable risk management concerns with respect to access, including due to inadequate data security; when a developer interface is unavailable; when there is insufficient information to authenticate a consumer or third party; when the scope of requested data is unclear; or when a consumer has revoked a third party's authorization.

The proposed rule would also encourage adoption of industry standards by treating conformance with a "qualified industry standard" as indicia (and, in one instance, conclusive evidence) of compliance with the proposed rule. A qualified industry standard would be one that is issued by a CFPB-recognized standard-setting body that satisfies requirements as to fairness, openness, and inclusion.

Finally, the timing for required compliance would be staggered. For depository institutions with over $500 billion in total assets, compliance would be required approximately six months following publication of the final rule in the *Federal Register*. The post-publication timing for required compliance would be extended to approximately one year for depository institutions with between $50 billion and $500 billion in total assets, to approximately 2.5 years for depository institutions with between $850 million and $50 billion in total assets, and to approximately four years for depository institutions with less than $850 million in total assets. For nondepository institutions, compliance would be required approximately six months post-publication for providers that generated $10 billion in revenue in the preceding calendar year or projected to do so in the current calendar year and approximately one year post-publication for other nondepository institutions.

A more detailed description of the proposed rule is included in Section III of this memorandum.

B. OBSERVATIONS

Outside the United States, regulatory requirements implemented in several jurisdictions over the past decade have meaningfully shaped processes for consumer-authorized financial data sharing and open banking ecosystems. Under the European Union's ("EU") second Payment Systems Directive (so-called "PSD2"), issued in 2015 and which remains in effect in substantial part in the United Kingdom post-Brexit, third parties that seek to access consumer data must be authorized by national authorities. In the United Kingdom, the Competition and Markets Authority directed large banks in 2017 to set up an entity, initially formed as the Open Banking Implementation Entity, to develop an open and common standard for an API (*i.e.*, a developer interface) that facilitates consumer-authorized access to banking data.

In contrast to the regulatory-driven approach in various jurisdictions outside the United States, development of consumer-authorized financial data sharing and open banking in the United States has been largely driven by market participants. These participants were responsible for the initial development of "screen scraping"—by which third parties obtain a consumer's log-in information and use that information to access the consumer's account—as a mechanism to access consumer financial data. Market participants have also been responsible for efforts to transition away from screen scraping, including through the formation of a standard-setting body seeking to develop common standards for developer interfaces and through bilateral agreements that have increasingly been entered into by large banks (which have typically acted as "data providers") and fintech providers and data aggregators (which have typically acted as "third parties") to govern information sharing through developer interfaces.

The CFPB's proposed rule, if finalized, would be the first set of generally applicable, prescriptive requirements targeting U.S. consumer-authorized data sharing and open banking. As a result, it could have significant implications for both market practices that have developed and future developments in this area, with substantial effects for consumers, data providers, third parties, and industry standards. Further, notwithstanding the potential broad effects of the proposed rule, there are several key issues that the CFPB does not address. Examples of potential key implications of the proposed rule include the following:

Consumer data access and portability rights. The proposed rule would grant U.S. consumers rights they do not currently have to access their personal financial data and to data portability, which are core elements of other federal and state privacy laws, such as the Health Insurance Portability and Accountability Act and the California Consumer Privacy Act of 2018. The Gramm-Leach-Bliley Act ("GLBA"), the federal privacy law that governs financial institutions, does not provide for such rights and state privacy and data protection laws generally do not apply to, or otherwise exempt, financial institutions and/or the information they collect. The proposed rule would therefore address this gap.[24] It would also put the United States in greater alignment with other jurisdictions that grant consumers rights to permit third-party access to their financial data, including the EU under the PSD2.

End of screen scraping. Screen scraping remains a common way for third parties to access consumer financial data and for data providers to make that data available. Indeed, the CFBP estimates that screen scraping represents approximately half of all third party data access (down from a large majority as recently as 2021).[25] The proposed rule would end screen scraping with respect to data providers, third parties, and data covered by the rule. This is in line with previous statements made by CFPB Director Chopra, in which he characterized screen scraping as causing the current open banking ecosystem to be "unstable."[26] The preamble to the proposed rule similarly describes screen scraping as potentially "compromis[ing] consumers' data privacy, security, and accuracy, as well as data provider interests related to security, liability, and risk management," including by putting "undue strain" on data provider information systems.[27] The proposed rule would not directly affect screen scraping of data that is not covered by the rule.

Fintech and data aggregator activities. The proposed requirements that third parties limit their collection, use, and retention of covered data to what is "reasonably necessary" to provide a consumer's requested product or service and re-solicit consumer authorization at least annually would impose meaningful restrictions not generally applicable today to fintechs, data aggregators, and others that access financial data with consumer authorization. The limits on collection, use, and retention would generally prohibit a third party from using covered data to support targeted advertising, cross-selling of other products or services, or selling covered data, even in circumstances where a customer may have expressly consented to these uses. These limits would also prohibit third parties from using de-identified data to the extent not reasonably necessary to provide a requested product or service to a consumer; the CFPB, however, has requested feedback on whether the final rule should permit third parties to solicit a consumer's opt-in consent to engage in such secondary uses with de-identified data. The requirement to obtain authorization at least annually could alleviate concerns raised by some observers that consumers may not understand the effect of their consent,[28] but could also, as the CFPB recognizes, increase customer attrition.[29]

The proposed rule would also require a third party, to be authorized to access covered data, to certify to consumers that it has an information security program that satisfies data security requirements imposed under the GLBA. Some third parties have denied or expressed uncertainty as to whether they are "financial institutions" within the meaning of the GLBA and therefore subject to these requirements, in particular, to apply the information security program required by the Federal Trade Commission's ("FTC") Standards for Safeguarding Customer Information, commonly referred to as the Safeguards Rule. For these third parties, the CFPB's approach would nonetheless require compliance with the Safeguards Rule, raising questions around how the CFPB would implement and enforce this requirement.

The CFPB also notes in the preamble that data aggregators that engage in certain tasks relating to assembling or evaluating data for the purpose of furnishing consumer reports to others may be regulated as "consumer reporting agencies" under the Fair Credit Reporting Act (the "FCRA").[30] A credit reporting agency is subject to various obligations, including with respect to disclosure, accuracy, consumer inspection, and disputes. Data aggregators should monitor the potential application of the FCRA in this

context, including in light of the CFPB's recent parallel announcement that it intends to propose new rules in 2024 that would, among other things, clarify when a "data broker" that sells certain types of consumer data is a credit reporting agency.[31]

Consequences of a security breach. The CFPB suggests that the proposed rule, in particular the required transition from access through screen scraping to access through developer interfaces, should reduce the effects of security breaches in connection with consumer-authorized financial data sharing.[32] The proposed rule would not eliminate the possibility of data breaches affecting covered data and the proposed rule does not address what should happen if a breach were to occur, including what, if any, actions an affected third party must take or how any resulting liability to affected consumers should ultimately be allocated between data providers and third parties. These issues may not be straightforward for data providers and third parties to resolve and may affect, for example, the negotiation of agreements that govern a third party's access to a data provider's developer interface; the CFPB appears to assume these agreements would be entered into.[33]

III. DETAILS OF THE PROPOSED RULE

The proposed rule would be codified in part 1033 of the CFPB's rules and divided into four subparts, lettered A through D. Subpart A would cover general matters, such as compliance dates, definitions, and the issuance of "qualified industry standards." Subpart B would address the obligation of "data providers" to make data available and the data covered by the proposed rule. Subpart C would address additional obligations that would apply to data providers, including the mechanics of making data available. Subpart D would cover requirements related to "third party" access to covered data, including access facilitated by "data aggregators."

The description of the proposed rule in this section is organized based on questions the proposal is likely to generate and answers to those questions. The questions are immediately below, hyperlinked to the relevant subsections of this memorandum where answers may be found.

What persons are within the scope of the proposed rule?

What data is within the scope of the proposed rule?

How would data providers satisfy their obligation to provide covered data?

What would be required of third parties who seek to access covered data?

In what circumstances would a data provider be permitted to refuse to provide data or impose access caps?

What would be qualified industry standards?

By when would compliance be required?

A. What persons are within the scope of the proposed rule?

Although the CFPB's rulemaking authority under section 1033 extends to all "covered persons," at least initially the proposed rule would extend obligations only to two subsets of covered persons engaged in particular activities. The first subset would be denominated "data providers" in the proposed rule. The second subset, which could potentially include parties that are not covered persons, would be referred to broadly as "third parties." "Data aggregators" would be a subset of third parties.

1. Data Providers

Reflecting the proposed rule's focus on payment- and payment account-related data, "data providers" would be defined as (1) financial institutions within the meaning of Regulation E (the CFPB's implementing regulations under the Electronic Fund Transfer Act);[34] (2) card issuers within the meaning of Regulation Z (the CFPB's implementing regulations under the Truth in Lending Act);[35] and (3) "[a]ny other person that controls or possesses information concerning a covered consumer financial product or service the consumer obtained from that person."[36] This third category would encompass a wide range of non-financial institutions, with digital wallet providers expressly included as an example. The proposed rule would include a limited exception for depository institutions that do not have a "consumer interface," as discussed below.[37] The CFPB recognizes in the preamble that covered persons typically share information concerning financial products and services other than the payment accounts and credit cards that are the focus of the proposed rule, such as mortgage, automobile, and student loans, and states that it intends to implement section 1033 with respect to other covered persons (and, as discussed below, other "consumer financial products or services") through supplemental rulemaking.[38]

2. Third Parties

Under the proposed rule, certain third parties would be able, with a consumer's authorization, to access the consumer's data from a data provider.[39] For this purpose, "third party" would be defined to mean "any person or entity that is not the consumer about whom the covered data pertains or the data provider that controls or possesses the consumer's covered data."[40] An "authorized third party" would be a third party that has complied with the authorization procedures discussed in subsection D.1 below.[41]

A "data aggregator," which would be defined as an entity that is "retained by and provides services to the authorized third party to enable access to covered data," would also be considered a third party.[42]

B. What data is within the scope of the proposed rule?

The proposed rule would require data providers to make available "covered data in the data provider's control or possession concerning a covered consumer financial product or service that the consumer obtained from the data provider."[43] Accordingly, the scope of data covered by the proposed rule turns on the meanings of "covered data" and "covered consumer financial product or service." The obligation to

provide covered data is subject to several enumerated exceptions, which are discussed in subsection E below.

1. Covered Data

The proposed rule would define "covered data"[44] to encompass six categories of information: (1) individual transaction information (both pending and historical); (2) account balance; (3) information to initiate payment to or from a Regulation E account (which include any checking, savings and similar account held primarily for personal, family or household purposes); (4) terms and conditions; (5) upcoming bill information; and (6) basic account verification information.[45] For the first category—transaction information—the obligation to provide all historical information in the data provider's possession or control would be subject to a "safe harbor" if at least 24 months of such information is provided.[46] For the third category—information to initiate a payment to or from a Regulation E account—the proposed rule would permit data providers to provide either or both of non-tokenized account and routing numbers and tokenized versions of the same information.[47] The proposed rule would include examples of data included in all but the second and final categories—account balance and basic account verification information. For the latter category, the data provider's obligation would be limited to providing the name, address, email address, and phone number associated with the covered consumer financial product or service.[48]

In complying with its obligation to provide covered data, a data provider would need to 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 debit card transactions.[49]

2. Covered Consumer Financial Products and Services

The CFPB's rulemaking authority under section 1033 extends to "consumer financial products or services," which the CFPA defines to mean generally "any financial product or service" listed in the CFPA that is "offered or provided for use by consumers primarily for personal, family, or household purposes[.]"[50] Listed financial products and services include a range of products and services provided to consumers, including "providing payments or other financial data processing products or services to a consumer by any technological means," subject to limited exclusions.[51]

Under the CFPA, the CFPB has the authority, including for purposes of section 1033, to identify additional "financial products or services" beyond those specifically listed in the CFPA.[52] Relying on that authority, the proposed rule would amend the CFPB's rules to include as a financial product or service "[p]roviding financial data processing products or services by any technological means, including processing, storing, aggregating, or transmitting financial or banking data, alone or in connection with another product or service."[53] The "another product or service" referred to in the last clause need not be financial, as acknowledged by the CFPB in the preamble.[54] Although the CFPB believes the activities encompassed by this amendment are already within the scope of activities listed in the CFPA, the codification is intended to provide "even greater certainty on this issue" and to "provide additional assurance that financial data

processing by third parties or others is subject to the CFPA and its prohibition on unfair, deceptive, and abusive acts or practices."[55]

For purposes of the proposed rule, the CFPB would initially limit the consumer financial products or services about which data providers must provide data to those that are "*covered* consumer financial products or services," which the CFPB would define to mean a consumer financial product or service that: (1) is a Regulation E account (*e.g.*, as noted above, a consumer checking or savings account);[56] (2) is a Regulation Z credit card;[57] or (3) facilitates payments from a Regulation E account or a Regulation Z credit card.[58] The third category is "intended to clarify that the proposed rule would cover all consumer-facing entities involved in facilitating the transactions the CFPB intends to cover."[59] As indicated above, the CFPB states in the preamble that it intends to implement section 1033 with respect to consumer financial products or services other than payment- and payment account-related products through supplemental rulemaking.[60]

C. How would data providers satisfy their obligation to provide covered data?

To satisfy their obligation to provide data, data providers would be required both to maintain a "consumer interface" and to establish and maintain a "developer interface."[61] Data providers would also be required to publish in a readily identifiable manner certain information about themselves to facilitate use of their developer interfaces, including identifying information, contact information, and information about their developer interfaces. Finally, data providers would be required to establish and maintain written policies and procedures in furtherance of the proposed rule. Each of these obligations is summarized below.

1. Interfaces

According to the CFPB, the separate requirements to maintain a consumer interface and to establish and maintain a developer interface would be intended in part to ensure that data providers do not rely on consumers sharing their log-in credentials with third parties and screen scraping by third parties of a consumer interface to satisfy their obligations under the proposed rule.[62]

For both types of interfaces, a data provider would be required to make covered data available in a machine-readable file that a consumer or authorized third party could retain and transfer into a separate information system.[63] In addition, a data provider would be prohibited from imposing any fees or charges for the interfaces or for receiving requests or providing covered data through the interfaces.[64] Accordingly, to the extent that data providers are currently charging such fees, the proposed rule would preclude them from doing so in the future.[65]

a. Consumer Interface

"Consumer interface" would be defined to mean an interface through which a data provider receives requests for covered data and makes available covered data in an electronic form usable *by consumers* in response to the requests.[66] A consumer interface generally would not satisfy a data provider's obligation to establish and maintain a developer interface.[67]

As long as a data provider satisfies the machine-readable file availability requirement through one of its consumer interfaces (*e.g.*, online banking or a mobile app), it may provide other consumer interfaces that do not satisfy that requirement.[68]

b. Developer Interface

Similarly, "developer interface" would be defined to mean an interface through which a data provider receives requests for covered data and makes available covered data in an electronic form usable *by authorized third parties* in response to the requests.[69] Developer interfaces would be required to satisfy several additional requirements related to format, performance, and security.

- Standardized Format. A developer interface would be required to make available covered data in a standardized format.[70] An interface would be deemed to satisfy this requirement if it makes covered data available in a format set forth in a qualified industry standard (the meaning of which is discussed in subsection F below)[71] or, in the absence of such a standard, in 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."[72] Notably, this is the one instance in which adherence to a qualified industry standard would provide a safe harbor and not merely constitute "indicia" of compliance with the relevant requirement of the proposed rule.
- Performance Standards. A data provider's developer interface would be required to perform at a "commercially reasonable" level.[73] Commercial reasonableness would be dictated by quantitative minimum performance specifications and additional specific indicia of commercial reasonableness. Subject to certain exclusions and conditions, the quantitative minimum performance specification would be a "response rate" of at least 99.5%.[74] The proposed rule would define "response rate" and certain related terms, including what qualifies as a "proper response" and a "commercially reasonable" amount of time to provide a response (no more than 3,500 milliseconds).[75] Indicia of performing at a commercially reasonable level would include: (1) whether the performance of the interface meets the applicable performance specifications set forth in a qualified industry standard; and (2) whether the performance meets the applicable performance specifications achieved by the developer interfaces established and maintained by similarly situated data providers.[76]
- Security Standards. Data providers would be required to implement several data security features in their consumer and developer interfaces.[77] In another provision aimed at eliminating screen scraping, data providers would be prohibited from allowing a third party to access the data provider's interface by using any credentials that a consumer uses to access the consumer interface.[78] In addition, data providers would be required to apply to their developer interfaces a data security program that satisfies the requirements of rules issued in furtherance of section 501 of the GLBA—rules commonly referred to as the GLBA Safeguards Framework.[79] For a data provider not subject to section 501, it would be required to apply the information security program required by the FTC's Safeguards Rule.[80]

2. Publication

To facilitate the ability of third parties to request covered data through a developer interface, the proposed rule would require data providers to publish certain information about themselves, including identifying information, contact information, and information about their developer interfaces, such as certain performance data.[81] The published information would need to be readily identifiable to members of the public in both human- and machine-readable formats. The publication requirements are intended, among other things, to enable standard-setting bodies to identify data providers and third parties participating in open banking and aid in efforts to develop qualified industry standards.[82]

- Identifying and Contact Information. A data provider would be required to publish its legal name and, if applicable, any assumed name it is using when doing business with the consumer; a link to its website; its Legal Entity Identifier ("LEI"); and contact information that would enable a consumer or third party to receive answers to questions about accessing covered data.[83]
- Developer Interface and Performance Information. A data provider would be required to publish documentation, including metadata describing all covered data and their corresponding data fields, sufficient for a third party to access and use its developer interface.[84] The published information would need to be maintained and updated as the developer interface is updated, include how third parties can get technical support and report issues, and be easy to understand and use.[85] Leveraging the performance standards referenced in subsection C.1.b above, a data provider would also be required to publish, on or before the tenth calendar day of each month, the percent of requests for covered data received by its developer interface in the preceding calendar month for which the interface provided a proper response.[86]

3. Policies and Procedures

Data providers would be required to establish and maintain written policies and procedures that are "reasonably designed to achieve the objectives" of the proposed rule related to covered data availability and data access.[87] The policies and procedures would need to be appropriate to the "size, nature, and complexity" of the data provider's activities and periodically reviewed and updated as appropriate to ensure their continued effectiveness.[88] In the preamble, the CFPB indicates that these requirements are intended to afford data providers "flexibility" to craft policies and procedures that are appropriate to the individual data provider rather than the policies and procedures that are appropriate to the industry at large; this flexibility, according to the CFPB, would also help data providers avoid conflicts with other legal obligations, manage data security risks, and minimize unnecessary impacts.[89] The required policies and procedures would need to address covered data availability, covered data accuracy, and record retention.

- Covered Data Availability. The policies and procedures would need to be reasonably designed to ensure that a data provider creates a record of the data fields that are covered data in its control or possession, what covered data are not made available through a consumer or developer interface pursuant to an exception (discussed in subsection E below), and the reason(s) the exception applies.[90] A data provider could comply with this requirement by incorporating the data fields defined by a qualified industry standard (discussed in subsection F below), but exclusive reliance on data fields defined by such a standard would not be appropriate if the data fields failed to identify all the covered data in the data provider's control or possession.[91] The policies and procedures would also need to address decisions to deny a third party access or a third party's or consumer's request for information, with the proposed rule specifying elements that must be included in the policies and procedures.[92]
- Covered Data Accuracy. The policies and procedures would need to be reasonably designed to ensure the accuracy of covered data made available through the data provider's developer interface. The proposed rule includes two examples of elements that data providers would need to consider: implementing the standardized format requirements described in subsection C.1.b above and addressing information provided by a consumer or a third party regarding inaccuracies in the covered data made available through its developer interface.[93] Indicia that a data provider's policies and procedures regarding accuracy are reasonable would include whether they conform to a qualified industry standard regarding accuracy.[94]
- Record Retention. The policies and procedures would need to be reasonably designed to ensure retention of records that evidence compliance with the data provider's obligations under the proposed rule related to covered data availability and data access.[95] The proposed rule would include a minimum retention period—three years—for records related to a data provider's response to a consumer's or

third party's request for information or a third party's request for access. All other records that are evidence of the data provider's compliance must be retained for a "reasonable period of time."[96] The proposed rule would identify particular categories of records that would need to be retained,[97] including records related to third party access to an interface, records related to requests for information, copies of a third party's authorization to access data on a consumer's behalf, and records of a consumer's revocation of a third party's access.[98]

D. What would be required of third parties to access covered data?

To become an "authorized third party," a third party would be required to satisfy authorization procedures set forth in the proposed rule, which would involve, among other things, the third party certifying to the consumer that it agrees to a series of obligations also set forth in the proposed rule. Certain additional requirements would apply when the third party is using a data aggregator. A third party that is a *covered person* or *service provider* would also be required to establish and maintain policies and procedures reasonably designed to ensure retention of records that evidence compliance with the requirements imposed on the third party by the proposed rule.[99]

1. Authorization Procedures

The proposed rule would implement a three-part authorization procedure for a third party to become an "authorized third party." Under those procedures, the third party would be required to: (a) provide the consumer with an authorization disclosure; (b) certify that the third party agrees to specific obligations; and (c) obtain the consumer's express informed consent to access covered data on behalf of the consumer.[100]

a. Authorization Disclosure

The third party would be required to provide the consumer with an authorization disclosure, electronically or in writing, that is clear, conspicuous, and segregated from other material.[101] The authorization disclosure would be required to include "key terms of access" set forth in the proposed rule, including, among other things, the certification statement and a description of the third party's revocation mechanism (each of which is described in subsection D.1.b below), but would not be required to take a particular form. The authorization disclosure would also need to include the name of any data aggregator that will assist the third party with accessing covered data and a brief description of the services the data aggregator will provide.[102] The authorization disclosure would be subject to certain language requirements.[103]

b. Certification Statement

As part of the authorization disclosure, a third party would be required to certify that the third party agrees to specific obligations set forth in the proposed rule.

- Reasonable Necessity. The third party would need to limit collection, use, and retention of covered data to what is "reasonably necessary" to provide the consumer's requested product or service.[104] According to the preamble, the "reasonably necessary" standard is "similar to standards in several data privacy frameworks that minimize third parties' collection, use, and retention of data,"[105] and the CFPB "will treat the product or service as the core function that the consumer sought in the market and that accrues to the consumer's benefit."[106] The proposed rule would identify targeted advertising, cross-selling of

other products or services, and the sale of covered data as "not part of, or reasonably necessary to provide, any other product or service[.]"[107] Third parties would be able to engage in those activities only to the extent a consumer sought to obtain them as "a stand-alone product."[108]

- Duration and Frequency. The third party would need to limit the duration of collection of covered data to a maximum period of one year after the consumer's most recent reauthorization.[109] To collect covered data beyond that period, the third party would need to obtain a new authorization from the consumer no later than the anniversary of the most recent authorization. The third party would be permitted to seek reauthorization in a "reasonable manner," with indicia of reasonableness including conformance to a qualified industry standard.[110] If the consumer does not provide a new authorization before the one-year period ends (and even if the consumer has not revoked the authorization), the third party could no longer: (1) collect covered data pursuant to the most recent authorization; or (2) use or retain covered data that was previously collected pursuant to the most recent authorization unless use or retention of that covered data remains "reasonably necessary" to provide the consumer's requested product or service.[111] The proposed rule would include examples of "reasonably necessary" uses, such as uses specifically required under other provisions of law, including to comply with subpoenas, protecting against fraud, and servicing or processing the product the consumer requested.[112] The preamble states that reasonable necessity would also include where there is "clear, affirmative indication [by the consumer] that they want to continue to use the product beyond the maximum period in a manner supported by the use and retention of data collected prior to expiration of that period."[113]

- Data Accuracy. The third party would need to establish and maintain written policies and procedures that are reasonably designed to ensure that covered data are accurately received from a data provider and accurately provided to another third party, if applicable.[114] These policies and procedures would be subject to the same "flexible" requirements and obligation to review and update as data provider policies and procedures.[115] The proposed rule would include two examples of elements that a third party would be required to consider when developing its policies and procedures: accepting covered data in the standardized format described in subsection C.1.b above and addressing information regarding inaccuracies in the covered data.[116] Indicia that a third party's policies and procedures are reasonable would include whether the policies and procedures conform to a qualified industry standard regarding accuracy.[117]

- Data security. Like data providers, the third party would need to apply an information security program that satisfies the applicable GLBA Safeguards Framework to their systems for the collection, use, and retention of covered data. A third party not subject to a GLBA Safeguards Framework would need to apply the information security program required by the FTC's Safeguards Rule.[118]

- Information Related to the Third Party and Its Access. The third party would need to provide the consumer with a copy of the consumer's authorization disclosure and provide readily identifiable contact information that enables a consumer to receive answers to questions about the third party's access to the consumer's covered data.[119] In addition, the third party would need to establish policies and procedures designed to ensure that, if asked by a consumer, the third party would provide the consumer the categories of covered data collected and the reasons for collecting it, the names of parties with which the covered data was shared and reasons for sharing, the status of the third party's authorization, and how the consumer can revoke the third party's access to the consumer's data.[120]

- Revocation Mechanism and Notification. The third party would need to provide the consumer with a mechanism to revoke the third party's authorization to access the consumer's data, and the mechanism would be required to be "easy to access and operate" and cost- and penalty-free.[121] According to the preamble, pursuant to this provision third parties would need to allow consumers to revoke consent to data access for a *particular* product or service, while maintaining consent to data access for any other products or services.[122] When a revocation request is received, the third party would need to notify the data provider, any data aggregator, and other third parties to whom the third party has provided the consumer's covered data.[123] Upon receipt of a revocation request, the third party could no longer: (1) collect covered data pursuant to the most recent authorization; or (2) use or retain covered data that was previously collected pursuant to the most recent authorization unless use or retention of that covered data remains reasonably necessary to provide the consumer's requested product or service, as discussed above.[124]

- Providing Covered Data to Others. Before providing covered data to another third party, the third party would need to require, by contract, the other third party to comply with the obligations described above, with the exception of those obligations specific to the third party's revocation mechanism, but including the obligations related to the effect of revocation.[125] Accordingly, any provision of covered data to another third party would be subject to the restriction that use of covered data be limited to what is reasonably necessary to provide the consumer's requested product or service requested.[126]

c. Express Informed Consent

To obtain express informed consent, the third party would need to obtain an authorization disclosure that is signed by the consumer electronically or in writing. As mentioned above, the third party would agree to provide the consumer with a copy of the consumer's authorization disclosure.

2. Policies and Procedures

In addition to the policies and procedures described in subsection D.1 above, the proposed rule would require a third party *that is a covered person or service provider*, as defined in the CFPA,[127] to establish and maintain policies and procedures reasonably designed to ensure retention of records that evidence compliance with the requirements imposed on the third party by the proposed rule.[128] Records would need to be maintained for a "reasonable period, not less than three years after a third party obtains the consumer's most recent authorization."[129] Much like a data provider, a third party would have flexibility to determine its policies and procedures in light of the size, nature, and complexity of its activities,[130] but certain specified records would be required: namely, the signed authorization disclosure and a record of actions taken by the consumer to revoke the third party's authorization as well as any data aggregator certification statement provided to the consumer.[131] A third party, like a data provider, would also be required to periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness.[132]

3. Data Aggregators

The proposed rule would allow, but not require, a data aggregator to perform the third party authorization procedures on behalf of a third party. The third party would remain responsible for compliance with the third party authorization procedures.[133] In addition, data aggregators would be required to comply with data aggregator-specific certification requirements. Specifically, the data aggregator would be required to certify to most of the matters that a third party must certify to, as detailed in subsection D.1.b above.[134] For this aggregator certification requirement to be satisfied, either the third party must include the aggregator certification in the authorization disclosure it provides the consumer, or the data aggregator must provide a separate certification to the consumer.[135] As mentioned above, the third party's authorization disclosure would need to include the name of any data aggregator that will assist the third party with accessing covered data and a brief description of the services the data aggregator will provide.[136] The third party would retain the flexibility to discontinue using a data aggregator or switch to a different aggregator.[137]

E. In what circumstances would a data provider be permitted to refuse to provide data or impose access caps?

The proposed rule would include a number of exceptions from the general obligation to provide covered data to a consumer or authorized third party. These exceptions fall into two categories: (1) exceptions tied to the nature of the covered data; and (2) exceptions tied to interface access. At the same time, a data provider would be prohibited from unreasonably restricting the frequency with which it receives and responds to requests for covered data through the use of "access caps" or "rate limits."

1. Exceptions Tied to the Nature of Covered Data

The proposed rule would include four categories of covered data that a data provider would not be required to make available to a consumer or authorized third party: (a) confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors;[138] (b) information collected by a data provider for the sole purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct;[139] (c) information required to be kept confidential by any other provision of law;[140] and (d) information that a data provider cannot retrieve in the ordinary course of its business with respect to that information.[141] These four exceptions are statutorily excluded from the data access right under section 1033 of the CFPA[142] and, according to the preamble, they are "narrow" and the CFPB intends to monitor the market for their pretextual use.[143]

2. Exceptions Tied to Interface Access

The proposed rule would also include several circumstances tied to interface access in which a data provider would not be required to make covered data available to a consumer or authorized third party. Denials of access related to risk management, insufficient evidence regarding the adequacy of a third party's data security practices, or a third party's failure to make public specified information about itself would be subject to a "reasonableness" standard, meaning that access could not be denied if the denial is unreasonable.

- Interface Unavailability. A data provider would not be required to make covered data available if its interface is not available when the data provider receives a request.[144]
- Insufficient Consumer Authentication. A data provider would not be required to make covered data available when a consumer or a third party is seeking the data and the data provider has not received information sufficient to authenticate the consumer's identity.[145] According to the preamble, consumers should be able to provide such information through procedures in use by most consumer interfaces that automatically authenticate consumers and allow consumers to identify covered data.[146]
- Insufficient Information About the Data Requested. A data provider would not be required to make covered data available when a consumer or a third party is seeking the data and the data provider has not received information sufficient to identify the scope of the data requested.[147] Again, consumers should be able to provide such information through procedures in use by most consumer interfaces that allow consumers to identify covered data.[148] Data providers would be permitted to ask the consumer to confirm the account(s) to which the third party is seeking access and the categories of covered data that will be accessed, including by presenting that information—as it is disclosed by the third party on the authorization disclosure—back to the consumer.[149]

- Insufficient Third Party Authentication. A data provider would not be required to make available covered data to a requesting third party acting on behalf of a consumer when the data provider has not received information sufficient to authenticate the third party's identity—*e.g.*, using an access token[150]—and confirm the third party has followed the authorization procedures applicable to third parties discussed in subsection D.1.[151]
- Risk Management Concerns. A data provider would be permitted to deny a consumer or third party access to an interface based on risk management concerns, provided the denial is reasonable.[152] To be reasonable, a denial would need to, at a minimum, be directly related to a specific risk of which the data provider is aware, such as a failure of the third party to maintain adequate data security, and would need to be applied in a consistent and non-discriminatory manner.[153] Subject to this requirement, a denial would not be unreasonable "if it is necessary to comply with the safety and soundness requirements or data security requirements in Federal law."[154] Indicia that a denial is reasonable would include whether the access is denied pursuant to the terms of a qualified industry standard related to data security or third party risk management.[155]
- Insufficient Information About the Third Party. Provided the data provider is acting reasonably, it would be able to deny a third party access to a developer interface if the third party fails to provide evidence that its data security practices are adequate to safeguard the covered data[156] or make available publicly certain identifying and contact information specified in the proposed rule.[157] The public disclosure of this information would be intended, among other things, to enable standard-setting bodies to identify data providers and third parties participating in the open banking system and standard-setting body efforts to develop industry standards.[158]
- Authorization Revoked. A data provider would not be required to make covered data available when a consumer has revoked authorization. The proposed rule would permit (but not require) a data provider to make available to the consumer a "reasonable method" by which the consumer may revoke a third party's authorization to access "*all* of the consumer's covered data."[159] Unlike the revocation mechanism a third party would be *required* to make available, described in subsection D.1.b above, a data's provider optional revocation method could not permit selective revocation. The proposed rule would include several non-exhaustive requirements to ensure an optional revocation method is reasonable,[160] with indicia of reasonableness including conformance of the method to a qualified industry standard.[161] A data provider that receives a revocation request from a consumer through the method would be required to notify the authorized third party of the request.

3. Access Caps or Rate Limits

A data provider would be prohibited from unreasonably restricting the frequency with which it receives and responds to requests for covered data *from an authorized third party* through the data provider's developer interface, including through the use of "access caps" or "rate limits."[162] This prohibition would be subject to the exceptions referenced in subsection E.1 and several of the exceptions referenced in E.2 above.[163] According to the preamble, those exceptions would allow restrictions only if they reasonably target a limited set of circumstances in which a third party requests information in a manner that poses an unreasonable burden on the data provider's developer interface and impacts the interface's availability to other authorized third party requests.[164] Any frequency restrictions would need to be applied in a manner that is non-discriminatory and consistent with the policies and procedures that the data provider would be required to establish and maintain, as described in subsection C.3 above. Indicia that any frequency restrictions applied are reasonable would include that they adhere to a qualified industry standard.[165]

F. What would be qualified industry standards?

The CFPB proposes throughout the proposed rule that conformance to a qualified industry standard would be indicia (and, in the case of standardized data format, conclusive evidence) of compliance with provisions of the proposed rule.[166] The proposed rule would define "qualified industry standard" to mean a standard issued by a standard-setting body that is fair, open, and inclusive in accordance with criteria specified in the proposed rule. Under the proposed rule, this would occur when the body has: (1) openness (sources, procedures, and processes used are open to all interested parties, including data providers, authorized third parties, data aggregators, relevant trade associations, as well as consumer and other public interest groups); (2) balance (decision-making power is balanced across all interested parties); (3) due process (use of documented and publicly available policies and procedures, adequate notice of meetings and standards development, sufficient time to review drafts, access to participant views, and fair and impartial conflict resolution); (4) an impartial appeals process; (5) consensus (standards are developed through consensus); (6) transparency (procedures or processes for participating in standards development and for developing standards are transparent to participants and publicly available); and (7) recognition by the CFPB within the last three years as an issuer of qualified industry standards.[167] The proposed rule would permit a standard-setting body to seek the CFPB's recognition as an issuer of qualified industry standards.[168]

With the exception of standardized data format, adherence to a qualified industry standard would neither be a safe harbor nor give rise to any presumption of compliance.[169] According to the preamble, the CFPB intends to "subsequently provide guidance on the substance of the standards issued by the qualified industry standard-setting bodies recognized by the CFPB."[170]

G. By when would compliance be required?

The establishment of any final rule and the amendment to the CFPB's existing rules to include financial data processing products or services as a financial product or service would take effect 60 days after the date of the final rule's publication in the *Federal Register*.[171] The proposed rule would provide for staggered compliance dates for data providers based on asset size or revenue, depending on the type of data provider.

The first compliance date would occur approximately six months after publication of the final rule in the *Federal Register* and would apply to depository institutions that hold at least $500 billion in total assets, and to nondepository institutions that generate at least $10 billion in revenue in the preceding calendar year or are projected to generate at least $10 billion in revenue in the current calendar year.[172] The second compliance date would occur approximately one year after *Federal Register* publication and would apply to depository institutions that hold at least $50 billion in total assets but less than $500 billion in total assets and to nondepository institutions that generate less than $10 billion in revenue in the preceding calendar year and are projected to generate less than $10 billion in revenue in the current calendar year.[173] The third compliance date would occur approximately 2.5 years after *Federal Register* publication and would apply

to depository institutions that hold at least $850 million but less than $50 billion in total assets.[174] The fourth compliance date would occur approximately four years after publication in the *Federal Register* and would apply to depository institutions with less than $850 million in total assets.[175]

* * *

ENDNOTES

1 Required Rulemaking on Personal Financial Data Rights, 88 Fed. Reg. 74,796 (Oct. 31, 2023).

2 The CFPA is title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. 111-203, 124 Stat. 1376, 1955 (2010). Section 1033 is codified at 12 U.S.C. § 5533.

3 *See* CFPB Press Release, CFPB Proposes Rule to Jumpstart Competition and Accelerate Shift to Open Banking (Oct. 19, 2023), *available at* https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-jumpstart-competition-and-accelerate-shift-to-open-banking/.

4 *Id.*

5 *Id.*

6 CFPB Director Rohit Chopra, Prepared Remarks of CFPB Director Rohit Chopra on the Proposed Personal Financial Data Rights Rule (Oct. 19, 2023), *available at* https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-rohit-chopra-on-the-proposed-personal-financial-data-rights-rule/.

7 12 U.S.C. § 5481(6).

8 12 U.S.C. § 5533(a).

9 12 U.S.C. § 5533(d).

10 Request for Information Regarding Consumer Access to Financial Records, 81 Fed. Reg. 83,806, 83,806 (Nov. 22, 2016).

11 Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation (Oct. 18, 2017), *available at* https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

12 Bureau Symposium: Consumer Access to Financial Records, a Summary of the Proceedings, *available at* https://www.consumerfinance.gov/data-research/research-reports/bureau-symposium-consumer-access-financial-records-summary-proceedings/; *see* CFPB Events, CFPB Symposium: Consumer Access to Financial Records, *available at* https://www.consumerfinance.gov/about-us/events/archive-past-events/cfpb-symposium-consumer-access-financial-records/.

13 *See* Consumer Access to Financial Records, 85 Fed. Reg. 71,003 (Nov. 6, 2020).

14 *See* Rulemaking Docket, CFPB-2020-0034, *available at* https://www.regulations.gov/docket/CFPB-2020-0034.

15 E.O. 14036, Executive Order on Promoting Competition in the American Economy, July 9, 2021, *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/.

16 Questions for the Record, Committee on Banking, Housing, and Urban Affairs Nominations of The Honorable Gary Gensler and The Honorable Rohit Chopra (Mar. 2, 2021), *available at* https://www.banking.senate.gov/imo/media/doc/Chopra%20Resp%20to%20QFRs%203-2-211.pdf.

17 Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights: Outline of Proposals and Alternatives Under Consideration (Oct. 27, 2022), *available at* https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf. This report is referred to repeatedly in the commentary accompanying the proposed rule.

18 *See* 5 U.S.C. § 609(b).

ENDNOTES (CONTINUED)

19 Final Report of the Small Business Review Panel on the CFPB's Proposals and Alternatives Under Consideration for the Required Rulemaking on Personal Financial Data Rights (Mar. 30, 2023), *available at* https://files.consumerfinance.gov/f/documents/cfpb_1033-data-rights-rule-sbrefa-panel-report_2023-03.pdf.

20 Proposed Rule, 88 Fed. Reg. at 74,802.

21 *See, e.g.*, Director Chopra's Prepared Remarks at Money 20/20 (Oct. 25, 2022), *available at* https://www.consumerfinance.gov/about-us/newsroom/director-chopra-prepared-remarks-at-money-20-20/; U.S. Dep't of the Treasury, Remarks by Assistant Secretary for Financial Institutions Graham Steele on the Digitization of Financial Services at the Transform Payments USA 2023 Conference (June 13, 2023), *available at* https://home.treasury.gov/news/press-releases/jy1530.

22 In the preamble, the CFPB states that it also held outreach meetings, met with advisory committees, consulted with staff from the prudential regulators and the Federal Trade Commission, and met with foreign counterparts. Proposed Rule, 88 Fed. Reg. at 74,802. Consultation with the federal banking agencies and FTC is required under section 1033. 12 U.S.C. § 5553(e).

23 Among numerous others, example providers of these services include Personal Capital and Quicken (personal financial management), Cash App and Venmo (payment applications), ApplePay and GooglePay (digital wallets), SoFi and Petal (credit underwriting, including cashflow underwriting), and Plaid and Envestnet|Yodlee (data aggregators, which also provide identity verification).

24 *See, e.g.*, 42 U.S.C. § 1320d-8 (Health Insurance Portability and Accountability Act); Cal. Civ. Code § 1798.145(e) (California Consumer Privacy Act).

25 Proposed Rule, 88 Fed. Reg. at 74,798.

26 Director Chopra's Prepared Remarks at Money 20/20 (Oct. 25, 2022), *available at* https://www.consumerfinance.gov/about-us/newsroom/director-chopra-prepared-remarks-at-money-20-20/.

27 Proposed Rule, 88 Fed. Reg. at 74,799.

28 For example, former Federal Reserve Board Governor Lael Brainard described that "when a consumer deletes a fintech app from his or her phone, it is not clear this would guarantee that a data aggregator would delete the consumer's bank login and password, nor discontinue accessing transaction information." Board of Governors of the Federal Reserve System, Governor Lael Brainard, Where Do Consumers Fit in the Fintech Stack? (Nov. 16, 2017), *available at* https://www.federalreserve.gov/newsevents/speech/brainard20171116a.htm.

29 Proposed Rule, 88 Fed. Reg. at 74,851. The CFPB's proposed annual reauthorization requirement would be less frequent for third parties than current requirements in the European Union and United Kingdom, which generally require consumer reauthorization or consent no less frequently than every 180 days (in the EU) or 90 days (in the UK).

30 Proposed Rule, 88 Fed. Reg. at 74,801.

31 *See* Remarks of CFPB Director Rohit Chopra at White House Roundtable on Protecting Americans from Harmful Data Broker Practices (Aug. 15, 2023), *available at* https://www.consumerfinance.gov/about-us/newsroom/remarks-of-cfpb-director-rohit-chopra-at-white-house-roundtable-on-protecting-americans-from-harmful-data-broker-practices/.

32 Proposed Rule, 88 Fed. Reg. at 74,858.

33 Proposed Rule, 88 Fed. Reg. at 74,849.

34 *See* 12 C.F.R. § 1005.2(i).

35 *See* 12 C.F.R. § 1026.2(a)(7).

36 Proposed Rule section 1033.111(c)(3).

ENDNOTES (CONTINUED)

37 *See* Proposed Rule section 1033.111(d). *See also* Proposed Rule, 88 Fed. Reg. at 74,804-06.

38 Proposed Rule, 88 Fed. Reg. at 74,804.

39 Proposed Rule, 88 Fed. Reg. at 74,807.

40 Proposed Rule section 1033.131; Proposed Rule, 88 Fed. Reg. at 74,807.

41 Proposed Rule section 1033.131; Proposed Rule, 88 Fed. Reg. at 74,807. The authorization procedures would be set forth in section 1033.401.

42 Proposed Rule section 1033.131.

43 Proposed Rule section 1033.201(a).

44 The proposed rule uses the term "covered data," instead of the statutory term "information."

45 Proposed Rule section 1033.211.

46 Proposed Rule, 88 Fed. Reg. at 74,810-11.

47 Proposed Rule section 1033.211(c).

48 Proposed Rule section 1033.211(f).

49 Proposed Rule section 1033.201(b).

50 *See* 12 U.S.C. § 5481(5).

51 12 U.S.C. § 5481(15)(A)(vii). *See also* 12 U.S.C. § 5481(15)(A)(ix).

52 *See* 12 U.S.C. § 5481(15)(A)(xi). The CFPA empowers the CFPB to do so where it finds the financial product or service is "permissible for a bank or for a financial holding company to offer or to provide under any provision of a Federal law or regulation applicable to a bank or a financial holding company, and has, or likely will have, a material impact on consumers." 12 U.S.C. § 5481(15)(A)(xi)(II). According to the preamble, the activities in proposed section 1001.2(b) are permissible for financial holding companies under the Federal Reserve Board's Regulation Y and for national banks under OCC regulations, and the processing of personal financial information has, or is likely to have, a material impact on consumers. Proposed Rule, 88 Fed. Reg. at 74,843.

53 Proposed Rule section 1001.2(b). The proposed rule does not purport to modify the statutory exclusions. Specifically, 12 U.S.C. § 5481(15)(A)(vii) provides that a person shall not be deemed to be a covered person with respect to financial data processing solely because the person engages in certain narrowly proscribed processing activities. CFPA section 1002(15)(A)(vii)(I) excludes as covered persons certain merchants, retailers, or sellers of non-financial products or services that are solely engaged in certain activities related to initiating payment instructions, whereas CFPA section 1002(15)(A)(vii)(II) excludes persons that solely provide access to a host server for websites. Proposed Rule, 88 Fed. Reg. at 74,843.

54 Proposed Rule, 88 Fed. Reg. at 74,843.

55 Proposed Rule, 88 Fed. Reg. at 74,800-01, 74,842-43.

56 *See* 12 C.F.R. § 1005.2(b).

57 *See* 12 C.F.R. § 1026.2(a)(15)(i).

58 Proposed Rule section 1033.111(b)(1) through (3). *See also* Proposed Rule, 88 Fed. Reg. at 74,803-04. The CFPB states in the preamble that it prioritized Regulation E accounts, Regulation Z credit cards, and payment facilitation products and services because the data supports payment facilitation and transaction-based underwriting across a range of markets. Proposed Rule, 88 Fed. Reg. at 74,804. The CFPB also acknowledges that electronic benefit transfer ("EBT") cards are exempt from EFTA coverage by statute and states that it is considering whether to add EBT-related data to the final rule or address EBT cards in a later rulemaking. *Id.*

59 Proposed Rule, 88 Fed. Reg. at 74,803.

ENDNOTES (CONTINUED)

60 Proposed Rule, 88 Fed. Reg. at 74,804.

61 Proposed Rule, 88 Fed. Reg. at 74,813.

62 Proposed Rule, 88 Fed. Reg. at 74,813.

63 Proposed Rule, 88 Fed. Reg. at 74,814.

64 Proposed Rule section 1033.301(c). *See also* Proposed Rule, 88 Fed. Reg. at 74,814-15.

65 Proposed Rule, 88 Fed. Reg. at 74,849.

66 Proposed Rule section 1033.131. As mentioned previously, the proposed rule would exclude data providers that do not have a consumer interface from the requirements of the proposed rule. Accordingly, the proposed rule would not require a data provider to establish a consumer interface, but only to maintain one it already has. Proposed Rule, 88 Fed. Reg. at 74,813.

67 Proposed Rule, 88 Fed. Reg. at 74,813.

68 Proposed Rule, 88 Fed. Reg. at 74,813.

69 Proposed Rule section 1033.131.

70 Proposed Rule section 1033.311(b).

71 Proposed Rule section 1033.311(b)(1).

72 Proposed Rule section 1033.311(b)(2).

73 Proposed Rule section 1033.311(c)(1).

74 Proposed Rule section 1033.311(c)(1)(i).

75 *Id.*

76 Proposed Rule section 1033.311(c)(1)(ii).

77 Proposed Rule, 88 Fed. Reg. at 74,818.

78 Proposed Rule section 1033.311(d)(1).

79 Proposed Rule section 1033.311(d)(2)(i). These rules (the GLBA Safeguards Framework) were published by the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of Thrift Supervision in 2001, after extensive industry comment, and have been regarded as successful in ensuring the security of customer information.

80 Proposed Rule section 1033.311(d)(2)(ii). The FTC Safeguards Rule, which took effect in 2003 and was most recently updated in 2023, imposes more prescriptive and specific information security requirements than the GLBA Safeguards Framework.

81 Proposed Rule, 88 Fed. Reg. at 74,825.

82 Proposed Rule, 88 Fed. Reg. at 74,825.

83 Proposed Rule section 1033.341(b). The preamble also identifies “the State in which they are incorporated” as among the identifying information data providers would be required to publish. Proposed Rule, 88 Fed. Reg. at 74,826. State of incorporation does not appear in the text of the proposed rule.

84 Proposed Rule section 1033.341(c).

85 *Id.*

86 Proposed Rule section 1033.341(d).

87 Proposed Rule section 1033.351(a).

88 *Id.*

ENDNOTES (CONTINUED)

89 Proposed Rule, 88 Fed. Reg. at 74,828.

90 Proposed Rule section 1033.351(b).

91 *Id.*

92 *Id.*

93 Proposed Rule section 1033.351(c).

94 *Id.*

95 Proposed Rule section 1033.351(d).

96 *Id.*

97 Proposed Rule, 88 Fed. Reg. at 74,829.

98 Proposed Rule section 1033.351(d)(2).

99 Proposed Rule section 1033.441(a).

100 Proposed Rule section 1033.401. For a jointly held account, a third party would have to comply with the third party authorization procedures in section 1033.401 of the Proposed Rule for the joint account holder on whose behalf the third party is requesting access. Proposed Rule, 88 Fed. Reg. at 74,830.

101 Proposed Rule section 1033.411(a).

102 Proposed Rule section 1033.431(b).

103 Proposed Rule section 1033.411(c).

104 Proposed Rule section 1033.421(a)(1).

105 Proposed Rule, 88 Fed. Reg. at 74,832.

106 Proposed Rule, 88 Fed. Reg. at 74,833.

107 Proposed Rule section 1033.421(a)(2).

108 Proposed Rule, 88 Fed. Reg. at 74,833 n.130.

109 Proposed Rule section 1033.421(b)(1), (2).

110 Proposed Rule section 1033.421(b)(3).

111 Proposed Rule section 1033.421(b)(4).

112 Proposed Rule section 1033.421(c).

113 Proposed Rule, 88 Fed. Reg. at 74,836.

114 Proposed Rule section 1033.421(d).

115 *Id.*

116 *Id.*

117 *Id.*

118 Proposed Rule section 1033.421(e).

119 Proposed Rule section 1033.421(g).

120 Proposed Rule section 1033.421(g)(3).

121 Proposed Rule section 1033.421(h)(1).

122 Proposed Rule, 88 Fed. Reg. at 74,840.

ENDNOTES (CONTINUED)

123 Proposed Rule section 1033.421(h)(2).

124 Proposed Rule section 1033.421(h)(3).

125 Proposed Rule section 1033.421(f).

126 Proposed Rule, 88 Fed. Reg. at 74,838.

127 *See* 12 U.S.C. § 5481(6) and (26).

128 Proposed Rule section 1033.441(a).

129 Proposed Rule section 1033.441(b).

130 Proposed Rule section 1033.441(c).

131 Proposed Rule section 1033.441(e).

132 Proposed Rule section 1033.441(d).

133 Proposed Rule section 1033.431(a).

134 Proposed Rule section 1033.431(c).

135 *Id.*

136 Proposed Rule section 1033.431(b).

137 Proposed Rule, 88 Fed. Reg. at 74,841.

138 Proposed Rule section 1033.221(a). Information, including annual percentage rate and other pricing terms, would not qualify for this exception merely because it is an input to, or an output of, an algorithm, risk score, or predictor. *Id.*

139 Proposed Rule section 1033.221(b). Information, such as name and other basic account verification information, collected for other purposes does not fall within this exception. *Id.*

140 Proposed Rule section 1033.221(c).

141 Proposed Rule section 1033.221(d).

142 12 U.S.C. § 5533(b).

143 Proposed Rule, 88 Fed. Reg. at 74,812-13.

144 Proposed Rule section 1033.331(c)(3). The exception that would permit a data provider to not make covered data available when its interface is not available would not affect the data provider's obligation (described above in subsection C.1) for its developer interface to perform at a commercially reasonable level, including by maintaining a "response rate" of at least 99.5%.

145 Proposed Rule section 1033.331(a), (b).

146 Proposed Rule, 88 Fed. Reg. at 74,822. Note, this particular exception would be couched as an affirmative obligation of the data provider to provide covered data when it receives the specified information.

147 Proposed Rule section 1033.331(a), (b).

148 Proposed Rule, 88 Fed. Reg. at 74,822. Note, this particular exception would be couched as an affirmative obligation of the data provider to provide covered data when it receives the specified information.

149 Proposed Rule section 1033.331(b)(2); Proposed Rule, 88 Fed. Reg. at 74,823.

150 Proposed Rule section 1033.331(b)(1)(ii); Proposed Rule, 88 Fed. Reg. at 74,823.

151 Proposed Rule section 1033.331(b)(1). According to the preamble, this step would generally be satisfied where the data provider receives a copy of the authorization disclosure the third party

provided to the consumer and that the consumer has signed. Proposed Rule, 88 Fed. Reg. at 74,823.

152 Proposed Rule, 88 Fed. Reg. at 74,819.

153 Proposed Rule section 1033.321(b).

154 Proposed Rule, 88 Fed. Reg. at 74,820.

155 Proposed Rule section 1033.321(c).

156 Proposed Rule section 1033.321(d). Where the third party does not present such evidence, the data provider may deny access under proposed § 1033.321(a) without vetting the third party. Where the third party does present such evidence, the data provider may either grant access or perform additional due diligence on the third party as appropriate. Proposed Rule, 88 Fed. Reg. at 74,821.

157 Proposed Rule section 1033.321(d).

158 Proposed Rule, 88 Fed. Reg. at 74,822.

159 Proposed Rule section 1033.331(e) (emphasis added).

160 Proposed Rule section 1033.331(e).

161 *Id.*

162 Proposed Rule section 1033.311(c)(2); Proposed Rule, 88 Fed. Reg. at 74,817.

163 Proposed Rule section 1033.331(c).

164 Proposed Rule, 88 Fed. Reg. at 74,817.

165 Proposed Rule section 1033.331(c)(2).

166 Proposed Rule, 88 Fed. Reg. at 74,807-08.

167 Proposed Rule section 1033.141(a).

168 Proposed Rule section 1033.141(b).

169 Proposed Rule, 88 Fed. Reg. at 74,807-08.

170 Proposed Rule, 88 Fed. Reg. at 74,808.

171 According to the preamble, because the activities covered by the amendment to part 1001 are already within the scope of the CFPA's definition of financial product or service, no compliance date applies. Proposed Rule, 88 Fed. Reg. at 74,843.

172 Proposed Rule section 1033.121(a).

173 Proposed Rule section 1033.121(b).

174 Proposed Rule section 1033.121(c).

175 Proposed Rule section 1033.121(d).

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 900 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.