BILLING CODE: 4810-AM-P

CONSUMER FINANCIAL PROTECTION BUREAU

12 CFR Parts 1001 and 1033

[Docket No. CFPB-2023-0052]

RIN 3170-AA78

Required Rulemaking on Personal Financial Data Rights

AGENCY: Consumer Financial Protection Bureau.

ACTION: Final rule.

SUMMARY: The Consumer Financial Protection Bureau (CFPB) is issuing a final rule to carry out the personal financial data rights established by the Consumer Financial Protection Act of 2010 (CFPA). The final rule requires banks, credit unions, and other financial service providers to make consumers' data available upon request to consumers and authorized third parties in a secure and reliable manner; defines obligations for third parties accessing consumers' data, including important privacy protections; and promotes fair, open, and inclusive industry standards.

DATES: This final rule is effective [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

Compliance dates: Data providers must comply with the requirements in subparts B and C beginning April 1, 2026; April 1, 2027; April 1, 2028; April 1, 2029; or April 1, 2030, depending on the criteria set forth in § 1033.121(c).

FOR FURTHER INFORMATION CONTACT: George Karithanom, Regulatory Implementation and Guidance Program Analyst, Office of Regulations, at 202-435-7700 or

https://reginquiries.consumerfinance.gov/. If you require this document in an alternative electronic format, please contact *CFPB_Accessibility@cfpb.gov*.

SUPPLEMENTARY INFORMATION:

Table of Contents

Abbreviations and Acronyms

ACH = Automated Clearing House

ANPR = Advance Notice of Proposed Rulemaking

API = Application programming interface

APR = Annual percentage rate

APY = Annual percentage yield

ATO = Account takeover

BLS = U.S. Bureau of Labor Statistics

BNPL = Buy Now Pay Later

EBT = Electronic benefit transfer

FDIC = Federal Deposit Insurance Corporation

FFIEC = Federal Financial Institutions Examination Council

FRFA = Final regulatory flexibility analysis

FTC = Federal Trade Commission

HHS = U.S. Department of Health and Human Services

IRFA = Initial regulatory flexibility analysis

LEI = Legal Entity Identifier

MSA = Metropolitan statistical area

NAICS = North American Industry Classification System

NCUA = National Credit Union Administration

NPRM = Notice of Proposed Rulemaking

OCC = Office of the Comptroller of the Currency (U.S. Department of the Treasury)

OFAC = Office of Foreign Assets Control (U.S. Department of the Treasury)

OMB = Office of Management and Budget (Executive Office of the President)

RFI = Request for Information

SBA = U.S. Small Business Administration

SBA Advocacy = U.S. Small Business Administration Office of Advocacy

SNAP = Supplemental Nutrition Assistance Program

SSN = Social Security number

TAN = Tokenized account number

URL = Uniform resource locator

USDA = U.S. Department of Agriculture

I. Overview

A. Summary of the Final Rule

When Congress established the Consumer Financial Protection Bureau in the Consumer Financial Protection Act (CFPA), it sought to ensure that markets for consumer financial products and services are fair, transparent, and competitive.[1] CFPA section 1033 lets consumers take action by giving them a right to access their account information and authorize certain third parties acting on their behalf to access that information. This right enables consumers to evaluate their account relationships and switch providers that are not benefiting them, and allows consumers to authorize third parties to access data on their behalf to provide valuable products and services they request. Increased competition can lead to innovation, attractive rates, quality service, and other benefits.

Specifically, CFPA section 1033(a) and (b) provide that, subject to rules prescribed by the CFPB, a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, subject to certain exceptions. The information must be made available in an electronic form usable by consumers. In addition, Congress mandated in section 1033(d) that the CFPB prescribe standards to promote the development and use of standardized formats for data made available under section 1033.

This final rule carries out these objectives by empowering consumers to access account data controlled by providers of certain consumer financial products or services in a safe, secure, reliable, and competitive manner. When implemented, consumers will be able to access their

[1] 12 U.S.C. 5511(a). The CFPA is title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. 111-203, 124 Stat. 1376, 2008 (2010).

own data and authorize third parties to access their data safely and with confidence that the third party is acting on their behalf, which means not collecting, using, or retaining consumer data for the benefit of entities other than the consumer. Consumers and authorized third parties will be able access data securely, ensuring that a baseline set of security standards apply across the market. They also will be able to access data reliably, promoting the accurate and consistent transmission of usable data. Consumer-authorized data access under the final rule also will occur in a manner that promotes competition through standardization and other measures to avoid entrenching incumbent data providers, intermediaries, and third parties that have commercial interests not always aligned with the interests of consumers and competition generally.

Coverage

In general, the final rule requires a "data provider" to make "covered data" about "covered financial products and services" available in electronic form to consumers and to certain "authorized third parties." For this purpose, an authorized third party is a third party that has complied with the authorization procedures set forth in subpart D of part 1033.

A "data provider" includes depository institutions (including credit unions) and nondepository institutions that issue credit cards, hold transaction accounts, issue devices to access an account, or provide other types of payment facilitation products or services. The final rule does not apply to certain small depository institutions as defined in the rule. In general, "covered data" includes information about transactions, costs, charges, and usage. This coverage is intended to prioritize some of the most beneficial use cases for consumers and leverage data providers' existing capabilities. Clarifying the scope of the data access right will also promote

consistency in the data made available to consumers, reduce costs of arranging for access to such data, and focus the development of technical standards around such data.

Access requirements

The final rule generally requires a data provider to make covered data available to consumers and authorized third parties upon request. The rule includes a number of functional requirements intended to ensure data providers make covered data available reliably, securely, and in a way that promotes competition. A data provider must make covered data available to authorized third parties in a standardized and machine-readable format and in a commercially reasonable manner, including by meeting a minimum response rate with respect to requests for covered data. A data provider must not unreasonably restrict the frequency with which it receives or responds to requests for covered data from an authorized third party. In addition, the data provider cannot comply with the requirement to make data available to authorized third parties by allowing the third party to engage in "screen scraping," an access method that uses consumer credentials to log in to consumer accounts to retrieve data.[2] The final rule also prohibits fees or charges related to consumer and third party data access. The final rule also requires a data provider to publicly disclose certain information about itself to facilitate access to covered data and to promote accountability.

The rule uses the term "developer interface" to refer to the functionality through which a data provider receives requests for covered data and makes the data available in electronic form usable by authorized third parties. Similarly, the rule uses the term "consumer interface" as a

[2] Unless otherwise stated, the term "screen scraping" in this final rule refers to credential-based screen scraping, which is prevalent in the market today.

label for the functionality with respect to consumer access. In neither case does the rule require the use of any particular technology.

Authorized third parties

To become an authorized third party, a third party must seek access to covered data on behalf of a consumer to provide a product or service that the consumer requested and: (1) provide the consumer with an authorization disclosure containing certain key terms of the data access; (2) provide a statement to the consumer in the authorization disclosure certifying that the third party agrees to certain obligations set forth in the final rule; and (3) obtain the consumer's express informed consent to access covered data on behalf of the consumer by obtaining an authorization disclosure that is signed by the consumer electronically or in writing.

Under the final rule, a third party must certify to limit its collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service. For purposes of this certification, targeted advertising, cross-selling, and the sale of covered data are not part of, or reasonably necessary to provide, any other product or service. The final rule includes examples of uses that are considered reasonably necessary to provide consumer requested products or services.

In addition to this general limit on collection, use, and retention of covered data, the third party also must certify to limit the duration of collection of covered data pursuant to a given authorization to a maximum period of one year. To continue collection, the third party must obtain a new authorization from the consumer no later than the anniversary of the most recent authorization. If a consumer does not provide a new authorization or if a consumer revokes authorization, the third party will cease its collection of covered data and cease its use and

retention of covered data that was previously collected unless use or retention of that covered data remains reasonably necessary to provide the consumer's requested product or service.

Under the final rule, a third party must also certify to:

- Have written policies and procedures that are reasonably designed to ensure that covered data are accurately received from a data provider and, if applicable, accurately provided to other third parties.
- Apply an information security program to its systems for the collection, use, and retention of covered data. Generally, the program must satisfy the applicable rules issued pursuant to the Safeguards Framework of the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. 6801 *et seq.* (GLBA Safeguards Framework).[3]
- Provide the consumer with a copy of the authorization disclosure that the consumer has signed electronically or in writing and contact information that enables a consumer to receive answers to questions about the third party's access to the consumer's covered data.
- Have reasonable written policies and procedures designed to ensure that the third party provides to the consumer, upon request, certain information about the third party's access to the consumer's covered data.

[3] The GLBA Safeguards Framework in this final rule refers the rules issued by the FTC and the guidelines issued by the prudential regulators that generally implement the GLBA's data security safeguards framework, pursuant to sections 501 (15 U.S.C. 6801) and 505 (15 U.S.C. 6805) of the GLBA. *See* Safeguards Rule, 16 CFR part 314; *Interagency Guidelines Establishing Standards for Safety and Soundness,* 12 CFR part 30, app. A (OCC); 12 CFR part 208, app. D-1 (Bd. of Governors of the Fed. Rsrv. Sys.); 12 CFR part 364, app. A (FDIC); and 12 CFR 748, app. A (NCUA). The GLBA Safeguards Framework sets forth standards for administrative, technical, and physical safeguards with respect to financial institutions' customer information. These standards generally apply to the security and confidentiality of customer records and information, anticipated threats or hazards to the security or integrity of such records, and unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

- Provide the consumer with a method to revoke the third party's authorization. Additionally, the third party will certify that it will notify the data provider, any data aggregator, and other third parties to which it has provided the consumer's covered data when the third party receives a consumer's revocation request.
- Require other third parties, by contract, to comply with specified third party obligations before providing covered data to them.

Data aggregators

The final rule permits data aggregators to perform the authorization procedures described in the final rule on behalf of the third party seeking the consumer's authorization. The third party seeking the consumer's authorization remains responsible for compliance with the authorization procedures even if it uses a data aggregator to perform the authorization procedures. If the third party will use a data aggregator to assist with accessing covered data, the data aggregator must certify to the consumer that it will satisfy the third party obligations discussed above (except the obligation to ensure consumers are informed, including the obligation to provide a copy of the authorization disclosure and contact information, and the obligation to provide a revocation mechanism), and this certification must be provided to the consumer. The third party may include this certification in the authorization disclosure or the data aggregator may provide it separately. Additionally, the third party's authorization disclosure must include the data aggregator's name and a description of the services that the data aggregator will provide in connection with accessing the consumer's covered data.

Policies and procedures, and recordkeeping for data providers and third parties

The final rule requires a data provider to have written policies and procedures that are reasonably designed to achieve certain objectives, including those related to what covered data

are generally made available, how a data provider responds to requests for developer interface access and requests for information, the accuracy of data transmitted through an interface, and record retention.

A third party that is a covered person or service provider as defined in the CFPA (12 U.S.C. 5481(6) and (26)), must establish and maintain written policies and procedures that are reasonably designed to ensure retention of records that are evidence of compliance for a reasonable period of time, not less than three years after a third party obtains the consumer's most recent authorization.

Financial products or services (part 1001)

The final rule defines financial products or services under the CFPA to ensure that it includes providing financial data processing. This provides 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.

B. Market Background

Digitization in consumer finance has the potential to facilitate more seamless consumer switching and greater competition. Consumers' ability to easily switch providers of consumer financial products and services creates strong competitive incentives that result in superior customer service and more favorable terms for consumers. Consumer-authorized sharing of personal financial data can produce positive market outcomes, but without appropriate safeguards it can also lead to misuse and abuse of consumer data.

Development of electronic data access and open banking

Most consumers with a bank account are enrolled in digital banking through online banking or mobile applications, and more than two-thirds use it as their primary method of

account access.[4] Consumer interfaces generally provide free access to information such as balances, transactions, and at least some terms of service. These consumer interfaces may provide additional functionality, such as allowing consumers to move money, manage their accounts, and download financial data.[5] Building on these developments, open banking[6] emerged in the early 2000s, along with interfaces designed for developers of products or services to request consumer information, and related industry standard-setting activity.[7] Third parties, such as personal financial advisors, often outsourced establishing and maintaining connections with data providers to data aggregators. These intermediaries largely relied on "screen scraping." Widespread screen scraping allowed open banking to grow quickly in the U.S. Screen scraping became a significant point of contention between third parties and data providers, in part due to its inherent risks, such as the proliferation of shared consumer credentials and overcollection of data.[8]

In recent years, the open banking system has continued to grow as consumer reliance on products and services powered by consumer-authorized data access has expanded. However, this

[4] Fed. Deposit Ins. Corp., *National Survey of Unbanked and Underbanked Households* (2021), https://www.fdic.gov/analysis/household-survey/2021report.pdf.

[5] For a more detailed discussion of the history of digital banking, *see* the NPRM, 88 FR 74796, 74797-98 (Oct. 31, 2023).

[6] This final rule generally uses the term "open banking" to refer to the network of entities sharing personal financial data with consumer authorization. Some stakeholders use the term "open finance" because of the role of nondepositories as important data sources. The CFPB views the two terms as interchangeable, but generally uses "open banking" because that term is more commonly used in the U.S.

[7] Maria Trombly, *Citibank's Aggregation Portal a Big Draw*, Computerworld (Sept. 18, 2000), https://www.computerworld.com/article/2597099/citibank-s-aggregation-portal-a-big-draw.html; Off. of the Comptroller of the Currency, *Bank-Provided Account Aggregation Services: Guidance to Banks* (2001), https://www.occ.treas.gov/news-issuances/bulletins/2001/bulletin-2001-12.html; CNET, *Net earnings: E-commerce in 1997* (Dec. 24, 1997), https://www.cnet.com/tech/tech-industry/net-earnings-e-commerce-in-1997/; Microsoft, *OFX Consortium Expands with Bank of America, Citigroup, Corillian, E*TRADE and TD Waterhouse* (Oct. 2, 2001), https://news.microsoft.com/2001/10/02/ofx-consortium-expands-with-bank-of-america-citigroup-corillian-etrade-and-td-waterhouse/.

[8] For a more detailed discussion of the history of screen scraping, *see* NPRM, 88 FR 74796, 74797-99 (Oct. 31, 2023).

growth has been uneven, with various disputes among system participants continuing to arise. Despite these challenges, financial institutions are dedicating more resources to developing open banking infrastructure, indicating significant consumer demand for open banking use cases, as well as interest among incumbents in maintaining some control over the system.

State of the open banking system

The CFPB estimates that, as of 2022, at least 100 million consumers had authorized a third party to access their account data. In 2022, the number of individual instances in which third parties accessed or attempted to access consumer financial accounts is estimated to have exceeded 50 billion and may have been as high as 100 billion, figures that vastly exceed the comparable public figures from some other jurisdictions' open banking systems, even on a per-capita basis.[9] These figures are likely to grow as consumer engagement continues and use cases expand.

The open banking system also engages a large number of entities, including thousands of depository institutions and third parties. A growing number of entities now serve as both data providers and third parties. For example, many depositories now act as third parties by offering personal financial management tools, while some entities offering so-called neobank accounts and digital wallets act as data providers. Most third party access is effectuated via a small number of aggregators, although some third parties elect to access at least some data directly.[10]

[9] *See* Press Release, Open Banking Ltd., *Open banking marks major milestone of 10 million users* (July 23, 2024), https://www.openbanking.org.uk/news/open-banking-marks-major-milestone-of-10-million-users/; and Consumer Data Right, *Performance, Overview, API Invocations*, https://www.cdr.gov.au/performance (scroll down to "Overview" dashboard; then, near the top right of dashboard, select "Date Slider"; then update date range from "1/1/2022" to "12/31/2022"; then view updated "API Invocations" data on the bottom left of dashboard) (last visited Oct. 16, 2024).

[10] For a more detailed discussion of the makeup of the market, *see* NPRM, 88 FR 74796, 74798 (Oct. 31, 2023).

Third party data access is generally enabled via screen scraping or developer interfaces.[11] Based on feedback received through public comments and stakeholder outreach, there is nearly universal consensus that safer forms of data access should supplant screen scraping.[12] However, to this point, such a transition has required data providers to choose to develop and maintain safer forms of data access, and required agreement between such providers and third parties on the resulting terms of data access, both of which have proved to be challenging propositions.[13] In spite of these challenges, open banking use cases continue to emerge and develop. Major use cases include personal financial management tools, payment applications and digital wallets, credit underwriting (including cashflow underwriting), and identity verification. While many major use cases began as innovative offerings by third parties, incumbent financial institutions have adopted many of them in response to consumer demand.

Challenges in the open banking system

Though the open banking system in the U.S. has grown considerably, significant challenges remain to achieving safe, secure, reliable, and competitive open banking. Divergent interests in the market with respect to the scope, terms, and mechanics of data access, and problems with the responsible collection, use, and retention of data have impeded the transition to safer forms of data access and the development of market-wide standards. This leads to inconsistent data access for consumers and market inefficiencies. These dynamics also impel third parties to rely on intermediaries, which have interests that may not always advance open banking since they stand to benefit from existing private network effects.

---

[11] For a more detailed discussion of these methods, *see id.*

[12] *See, e.g.*, Consumer Fin. Prot. Bureau, *Bureau Symposium: Consumer Access to Financial Records Report*, at 3-4 (July 2020), https://files.consumerfinance.gov/f/documents/cfpb_bureau-symposium-consumer-access-financial-records_report.pdf.

[13] For a more detailed discussion of this transition, *see* NPRM, 88 FR 74796, 74798-99 (Oct. 31, 2023).

Market participants' interests may diverge due to interrelated competitive, legal, and regulatory factors. For example, data providers may limit the data they share or refrain from sharing altogether to protect their market position, while third parties may collect more data than they reasonably need to provide the products or services sought by the consumer.[14] Such unnecessary collection, use, and retention of consumer data by third parties does not benefit consumers and needlessly encroaches on consumers' privacy interests.

Impacts of these challenges on the open banking system

The challenges described above have impeded progress on safer forms of data access and hampered multilateral efforts by industry to establish open banking standards.[15] This stasis has forced the open banking system to depend heavily on a handful of data aggregators that accrue economic benefits from the system's inability to scale safer forms of data access and open industry standards. Dependency on a handful of data aggregators creates incentives for them to rent-seek and self-preference. In a more open system where safer forms of data access are appropriately accessible and third parties are easily verified, third parties and data providers may choose to connect without intermediaries if they wish, or continue to use them to the extent they offer compelling value.

When the challenges impeding progress described above are resolved, consumers should be able to safely, securely, and reliably exercise their data access rights in a competitive open banking system not dominated by the interests of any one segment of the market.

[14] For a more detailed discussion of divergent interests present in the market and the risks created by particular practices, including screen scraping, *see id.* at 74798-99.

[15] For a more detailed discussion of how such progress has been hampered, *see id.* at 74799.

II. The Proposal and Other Procedural Background

A. Outreach

In addition to the industry and community outreach described in the proposal, [16] in 2016, the CFPB published in the *Federal Register* an RFI Regarding Consumer Access to Financial Information on topics including consumer-authorized data access[17] and in 2020 held a symposium with stakeholders[18] and published an ANPR in the *Federal Register*.[19] Pursuant to the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA),[20] the CFPB in 2022 issued its Outline of Proposals and Alternatives under Consideration for the Required Rulemaking on Personal Financial Data Rights (Outline or SBREFA Outline)[21] and in 2023 convened a SBREFA Panel,[22] which issued a report (Panel Report or SBREFA Panel Report).[23]

---

[16] *See* 88 FR 74796, 74799 (Oct. 31, 2023). This outreach included the issuance of two sets of market monitoring orders under CFPA section 1022(c)(4) (described in the proposed rule as the "Provider Collection" and "Aggregator Collection"), and engagement with CFPB advisory boards and committees.

[17] *See* 81 FR 83806 (Nov. 22, 2016). In 2017, the CFPB published a summary of comments received in response to the RFI and other stakeholder meetings. *See* Consumer Fin. Prot. Bureau, *Consumer-authorized financial data sharing and aggregation: Stakeholder insights that inform the Consumer Protection Principles* (Oct. 18, 2017), https://www.consumerfinance.gov/data-research/research-reports/consumer-protection-principles-consumer-authorized-financial-data-sharing-and-aggregation/.

[18] *See* Consumer Fin. Prot. Bureau, *Bureau Symposium: Consumer Access to Financial Records: A summary of the proceedings* (July 2020), https://files.consumerfinance.gov/f/documents/cfpb_bureau-symposium-consumer-access-financial-records_report.pdf.

[19] *See* 85 FR 71003 (Nov. 6, 2020).

[20] Pub. L. 104-121, 110 Stat. 857 (1996).

[21] Consumer Fin. Prot. Bureau, *Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights, Outline of Proposals and Alternatives under Consideration* (Oct. 27, 2022), https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf.

[22] The Panel consisted of a representative from the CFPB, the Chief Counsel for Advocacy of the Small Business Administration, and a representative from the Office of Information and Regulatory Affairs in OMB.

[23] Consumer Fin. Prot. Bureau, *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), https://files.consumerfinance.gov/f/documents/cfpb_1033-data-rights-rule-sbrefa-panel-report_2023-03.pdf. As required under the Regulatory Flexibility Act, the CFPB considered the Panel's findings in its IRFA, as set out in the NPRM. *See* 88 FR 74796, 74862 (Oct. 31, 2023). The CFPB considered the feedback it received from small entity representatives and the findings and recommendations of the Panel. The CFPB invited other stakeholders to submit feedback on the SBREFA Outline, which was not considered by the Panel and is not reflected in the Panel Report. *See* https://www.regulations.gov/document/CFPB-2023-0011-0001/comment.

In December 2023, CFPB staff met with the Consumer Advisory Board, the Community Bank Advisory Council, and the Credit Union Advisory Council to receive feedback on the proposed rule.[24]

Before and after issuing the proposal, CFPB staff met on numerous occasions to obtain feedback from staff from the Board of Governors of the Federal Reserve System, OCC, FDIC, NCUA, and FTC, including on the subjects in CFPA sections 1022(b)(2)(B) and 1033(e). CFPB staff has also met with staff from other Federal agencies, including staff from the USDA, the U.S. Department of the Treasury, the U.S. Department of Justice, the U.S. Department of Commerce, the Federal Housing Finance Agency, as well as staff from State agencies.

B. Summary of the Proposed Rule

On October 19, 2023, the CFPB released the Notice of Proposed Rulemaking for the Required Rulemaking on Personal Financial Data Rights. The proposal was published in the *Federal Register* on October 31, 2023, and the public comment period closed on December 29, 2023. *See* 88 FR 74796 (Oct. 31, 2023).

Part 1033

The proposal would have implemented CFPA section 1033 by ensuring consumers and third parties who are authorized to access covered data on behalf of consumers can access covered data in an electronic form from data providers. In general, the proposal sought to foster a data access framework that is safe, by ensuring third parties are acting on behalf of consumers when accessing their data, including with respect to consumers' privacy interests; secure, by applying a consistent set of security standards across the market; reliable, by promoting the

[24] This feedback was submitted to the rulemaking docket. *See* https://www.regulations.gov/comment/CFPB-2023-0052-11086 (Community Bank Advisory Council); https://www.regulations.gov/comment/CFPB-2023-0052-11087 (Credit Union Advisory Council); https://www.regulations.gov/comment/CFPB-2023-0052-11088 (Consumer Advisory Board).

accurate and consistent transmission of data that are usable by consumers and authorized third parties; and competitive, by promoting standardization and not entrenching the roles of incumbent data providers, intermediaries, and third parties whose commercial interests might not align with the interests of consumers and competition generally. The proposed rule sought to foster this kind of framework by direct regulation of practices in the market and by identifying areas in which fair, open, and inclusive standards can develop to provide additional guidance to the market. Consistent with the statutory mandate in CFPA section 1033(d), various provisions in the proposed rule sought to promote the use and development of standardized formats. The proposal identified six general objectives to be achieved by its various provisions.

First, the proposal would have clarified the scope of data access rights under CFPA section 1033 by defining key terms, establishing which covered persons would be required to make data available to consumers, and defining which data would need to be made available to consumers. Second, the proposal would have established basic standards for data access by requiring data providers to maintain a consumer interface for consumers and a developer interface for third parties to access consumer-authorized data under CFPA section 1033. Data providers would have been required to make available covered data to authorized third parties in a standardized format, in a commercially reasonable manner, without unreasonable access caps, and pursuant to certain security specifications. In addition, data providers would have had to follow certain procedures to disclose information about themselves and their developer interfaces, and to establish and maintain certain written policies and procedures to ensure compliance with the provisions of the rule and promote the objectives of CFPA section 1033. Third, the proposal would have prevented data providers from allowing a third party to access the system using consumer interface credentials. This and the proposals described above were

intended to transition the market from screen scraping towards an access method that complies with CFPA section 1033. Fourth, the proposal would have defined the mechanics of data access by proposing certain requirements and clarifications with respect to when a data provider must make available covered data upon request to consumers and authorized third parties. Fifth, the proposal sought to ensure third parties are acting on behalf of consumers through requirements that a third party certify to consumers that it will only collect, use, and retain the consumer's data to the extent reasonably necessary to provide the consumer's requested product or service. The proposed rule also sought to improve consumers' understanding of third parties' data practices by requiring a clear and conspicuous authorization disclosure including key facts about the third party and its practices. Other key protections in the proposed rule would have included limiting the length of data access authorizations and requiring deletion of consumer data in many cases when a consumer's authorization expires or is revoked. Sixth, the proposal sought to promote fair, open, and inclusive industry standards by proposing that conformance with "qualified industry standards" issued by standard-setting bodies recognized by the CFPB would provide some indicia of compliance with various rule provisions.

Part 1001

Separately, the proposed rule would have defined financial products or services under the CFPA in 12 CFR part 1001 to ensure that the definition includes providing financial data processing. The proposal explained that this would 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.

Comments

The CFPB received approximately 11,120 public comments on the proposal during the comment period.[25] Approximately 290 of these comments were unique, detailed comment letters. These commenters included data providers and third parties, including banks of different sizes, credit unions, a variety of nondepository entities, and data aggregators;[26] trade associations representing a diverse array of interests; standard-setting organizations;[27] consumer advocates;[28] researchers and a variety of research institutes; members of Congress; government agencies; law firms; and individual commenters not affiliated with or representing any organization.

In addition, the CFPB considered comments received after the comment period closed via approximately 60 ex parte submissions and meetings.[29] These materials, including all ex parte submissions and summaries of ex parte meetings, will be available on the public docket for this rulemaking.[30]

The remaining comments included some duplicate submissions (*i.e.*, letters with the same content from the same commenter submitted through multiple channels, or letters with the same content submitted by multiple people on behalf of the same commenting organization) as well as comments that appeared to be part of several comment submission campaigns. Such comment

[25] *See* https://www.regulations.gov/docket/CFPB-2023-0052/comments.

[26] Depending on the context and its activities, a particular entity might be a data provider, a third party, a data aggregator acting on behalf of a third party, or some combination thereof. The description of commenters in this final rule attempts to characterize the commenter based on the expressed or inferred capacity in which they provided feedback.

[27] As used in this final rule, this term refers to nonprofit entities that described themselves principally as industry standard-setting organizations. The CFPB recognizes, however, that a variety of other commenters might be involved in standard-setting activities.

[28] As used in this final rule, this term refers broadly to all types of consumer advocates, including privacy advocates and community groups.

[29] *See* Consumer Fin. Prot. Bureau, *Policy on Ex Parte Presentations in Rulemaking Proceedings*, 82 FR 18687 (Apr. 21, 2017).

[30] *See* https://www.regulations.gov/docket/CFPB-2023-0052.

campaigns typically advocated for or against particular provisions in the proposal and urged additional changes. These comments were considered by the CFPB along with all other comments received, including any additional remarks included in otherwise identical comment letters.

The CFPB received comments on nearly all aspects of the proposed rule, and on its analyses of the proposed rule's impacts. Relevant information received via comment letters, as well as ex parte submissions, is discussed below in subsequent parts of this document, as applicable. The CFPB considered all the comments it received regarding the proposal, made certain modifications, and is adopting the final rule as described in part IV below.

C. 2024 Industry Standard-Setting Final Rule

In June 2024, the CFPB finalized the proposal in part, establishing attributes a standard-setting body must possess to receive CFPB recognition for purposes of issuing standards that provide some indicia of compliance with certain substantive provisions of part 1033, as well as establishing the application process for CFPB recognition. *See* 89 FR 49084 (June 11, 2024) (Industry Standard-Setting Final Rule).

III. Legal Authority

A. CFPA Section 1033

CFPA section 1033(a) and (b) provide that, subject to rules prescribed by the CFPB, a covered person shall make available to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, subject to certain exceptions. The information must be made available in an electronic form usable by consumers. Section 1002 of the CFPA defines certain terms used in CFPA section 1033, including defining "consumer" as "an

individual or an agent, trustee, or representative acting on behalf of an individual." In light of these purposes and objectives of section 1033 and the CFPA generally, the CFPB interprets CFPA section 1033 as authority to establish a framework that ensures data providers readily make available to consumers and third parties acting on behalf of consumers (including authorized third parties offering competing products and services), upon request, covered data in a usable electronic form. In addition, CFPA section 1033(d) provides that the CFPB, by rule, shall prescribe standards applicable to covered persons to promote the development and use of standardized formats for information, including through the use of machine-readable files, to be made available to consumers under this section. Moreover, the CFPB interprets CFPA section 1033 as authority to specify procedures to ensure third parties are truly acting on behalf of consumers when accessing covered data. These procedures help ensure the market for consumer-authorized data operates fairly, transparently, and competitively.

CFPA section 1033(c) provides that nothing in CFPA section 1033 shall be construed to impose any duty on a covered person to maintain or keep any information about a consumer. Further, CFPA section 1033(e) requires that the CFPB consult with the prudential regulators and the FTC to ensure, to the extent appropriate, that certain objectives are met.

B. CFPA Sections 1022(b) and 1024(b)(7)

CFPA section 1022(b)(1) authorizes the CFPB to, among other things, prescribe rules "as may be necessary or appropriate to enable the [CFPB] to administer and carry out the purposes and objectives of the Federal consumer financial laws, and to prevent evasions thereof." The CFPA is a Federal consumer financial law.[31] Accordingly, in issuing the proposed rule, the CFPB is exercising its authority under CFPA section 1022(b) to prescribe rules that carry out the

[31] *See* 12 U.S.C. 5481(14) (defining "Federal consumer financial law" to include the provisions of the CFPA).

purposes and objectives of the CFPA and to prevent evasions thereof. This would include, at least in part, provisions to require covered persons or service providers to establish and maintain reasonable policies and procedures, such as those to create and maintain records that demonstrate compliance with the rule after the applicable compliance date. CFPA section 1024(b)(7) also grants the CFPB authority to impose record retention requirements on CFPB-supervised nondepository covered persons "for the purposes of facilitating supervision of such persons and assessing and detecting risks to consumers."

C. CFPA Section 1002

Certain provisions of the CFPA, such as its prohibition on unfair, deceptive, or abusive acts or practices, apply in connection with a consumer financial product or service. Under CFPA section 1002(5), this is generally defined as a financial product or service that is "offered or provided for use by consumers primarily for personal, family, or household purposes." In turn, CFPA section 1002(15) defines a financial product or service by reference to a number of categories. In addition, CFPA section 1002(15)(A)(xi)(II) authorizes the CFPB to issue a regulation to define as a financial product or service, for purposes of the CFPA, "such other financial product or service" that the CFPB finds 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." The CFPB is exercising this authority in finalizing § 1001.2(b).

IV. Discussion of the Final Rule

12 CFR Part 1033

General Comments Received on the Proposal

High-level and general comments received on the CFPB's proposed rule to implement CFPA section 1033 are discussed here, followed by a discussion of comments specifically addressing the rulemaking process, liability among commercial entities, and overlaps with other consumer financial laws and CFPB rulemaking activity. Comments received on specific aspects of the CFPB's proposed rule, as well as regarding the CFPB's legal authority to adopt specific aspects of the rule, and the anticipated effects of particular provisions, are discussed in turn in the sections that follow in this part IV. Comments regarding the CFPB's analysis of impacts are discussed in parts VI through VIII.

1. High-level and general comments on the proposal

General support

Most commenters, including data providers, third parties, data aggregators, trade associations, consumer advocates, and others, supported the overall goals of the rulemaking articulated in the proposal. Many commenters supported implementing the data access rights in CFPA section 1033 to include direct consumer and third party access that would allow consumers and authorized third parties to access data more reliably and securely compared to current market practices. A research institute commenter stated that the proposal would assure a robust regime of third party access with respect to its coverage, while building in flexibility to allow the regime to evolve along with changes in market standards and technology.

Many third party commenters, consumer advocates, and others stated consumer-authorized access would help consumers, including those underserved by their existing account

providers, manage their financial lives and access new and competing products and services. A community bank commenter indicated the proposal would help ensure community banks remain vital in the areas they serve.

Many commenters, including third parties, data providers, consumer advocates, and others also stated that the rule would generally increase competition overall by reducing barriers to entry and other impediments for market participants to compete with incumbent depository and nondepository institutions. For example, a credit union commenter stated that the standardization of third party data access would allow smaller institutions to rely on the same technology as larger institutions, decreasing incumbents' market power. Other commenters believed that the proposal's approach to standard-setting would reduce the influence of incumbents and increase consumers' bargaining power and access to services offered by different providers. Some data provider commenters stated that the proposal would support competition by limiting third party secondary use of consumer-authorized data and ensuring third parties are subject to a basic standard for data security.

Some commenters specifically indicated that the rule would have competitive benefits in certain markets. For example, a trade association for certain third parties stated that open banking can spur competition in the payments sector, lowering transaction costs and mitigating the durable market power of certain incumbents. The commenter noted that the proposal's prohibition on fees for third party access would allow cost-sensitive merchants to accept lower-cost payments.

Commenters also emphasized the benefits of informed consent and consumer control when sharing data with third parties and the need for consumer protection in consumer-authorized access. Many data providers, third parties, consumer advocates, and others also

supported the rule's efforts to protect consumers by enabling them to control their data effectively. For example, a consumer advocate expressed general support for the proposal, characterizing it as a strong, protective rule that would ensure that consumers can share account data free of misuse or exploitation. This commenter also stated the consumer protections in the rule should serve as a model for how to safeguard consumer control and privacy when a consumer grants permission to a business to use their data.

General opposition

While many commenters supported the proposal overall, some data providers, third parties, and others were critical of some or all aspects of the proposal. A number of data provider commenters, particularly credit unions and community banks, expressed opposition to the proposal as a whole, and questioned whether a rule was necessary or appropriate to achieve the CFPB's stated goals, including with respect to competition, and questioned the CFPB's legal authority to issue rules for open banking.

In addition, a wide variety of commenters, including data providers and third parties, raised what they described as significant concerns about the costs of the proposal, often with respect to specific provisions. In particular, data providers were most concerned with potential compliance costs related to the Fair Credit Reporting Act (FCRA), 15 U.S.C. 1681 *et seq.*, the costs of providing access to third parties in compliance with the rule as proposed (including the prohibition on charging fees for access), the costs associated with managing third party risk, and how liability would be allocated for third party breaches or fraud. A number of entities—mainly though not exclusively third parties that use consumer-authorized data—asserted that the proposed third party limitation on collection, use, and retention of covered data would foundationally undermine the rule and restrict consumers' ability to share their data. A large

number of smaller financial institutions and related trade associations expressed concern that the proposal would disadvantage small entities.

A variety of commenters suggested that the proposal would undermine competition in various ways. Some commenters, including research institutes, third parties, and data providers asserted that the proposal's coverage was too narrow to support competition. For example, a data aggregator stated that the proposal's limited coverage of products and data types would reduce third party innovation, and a research institute stated that the limited coverage of data providers would give them an incentive to block data access outside of the rule's coverage, further limiting third party access to data. A research institute and a data provider commenter stated that the proposal would undermine competition by limiting the role of industry standard-setting organizations that are not recognized by the CFPB.

Some credit union and community bank commenters stated that the rule as a whole would unfairly force data providers to maintain data access systems and bear other costs, effectively subsidizing competition from third parties, particularly as a result of the proposed fee prohibition for third party data access. Several of these commenters noted that this result would benefit nondepositories that are excluded from the data provider definition and would come at the expense of depository institutions, which would disproportionately disadvantage credit unions and community banks. Data providers expressed concern that they would unfairly bear the burden of managing liability risks presented by nondepository third parties that are not subject to the same regulatory oversight. Several data provider commenters expressed concern that third parties would use consumer data to harm data providers, such as by reverse-engineering sensitive commercial information. A data aggregator commenter stated that the proposal would

consolidate the market of data aggregators by forcing data providers to grant access to third parties, ultimately stifling innovation.

Credit union and community bank commenters also expressed concern that the proposal would disadvantage them relative to larger and better resourced data providers. These commenters stated that the proposal would impose disproportionate and unsustainable costs on smaller data providers and would force some to exit the market or otherwise consolidate the banking industry, reducing consumer access to products and services. A number of commenters stated that smaller depository institutions that rely on core service providers would be less able to manage the costs of a prohibition on fees for third party access. One data provider commenter stated that the proposed rule would force less-resourced data providers to adhere to standards established by the largest data providers, which would reduce their profitability. Another data provider commenter stated that forcing some data providers to make data available to third parties while exempting community banks would put community banks at a competitive disadvantage relative to large data providers.

As discussed in part IV.D.4, a variety of third party commenters expressed concern that the proposed limitation on collection, use, and retention of covered data would restrict innovation by third parties or limit the ability of new entrants and providers of new products and services to provide innovative products. For example, a trade association representing nondepository institutions argued that the final rule should allow broader use of covered data for advertising purposes to support competition, while numerous commenters, including research institutes and others, expressed concern about the limitation on use of de-identified data, including for research purposes. Other commenters argued the proposed limitation on collection, use, and retention of covered data would not only disadvantage third parties relative to other

market participants, but also reduce the competitiveness of the U.S. overall. Some commenters also asserted that the proposed third party obligations, including the limit on collection, use, and retention of covered data, would put third parties at a significant competitive disadvantage to data providers that are unrestricted by the limitations. For example, some commenters stated that the proposed limitation on a third party's duration of authorization would disadvantage third parties engaged in payments relative to incumbents that do not rely on consumer-authorized data. Some third party commenters also stated that the proposal's allowance of tokenized account numbers would result in anticompetitive conduct by data providers.

Several commenters argued that the market for consumer-authorized data is already competitive and that a rulemaking to increase competition among data providers, intermediaries, and third parties, would be unnecessary or would yield few benefits. As evidence of the level of competition in the U.S., commenters noted that third parties access (or attempt to access) consumer-authorized data more frequently in the U.S. than in other countries; noted that the market is already moving toward the use of APIs and away from screen scraping; and asserted that the market for data provider products and services (including for credit card and deposit accounts) is robust and provides high levels of customer service. Some commenters representing community banks asserted that consumers are not demanding third party data access, but that community banks would provide it if consumers did demand it.

Some commenters, particularly community banks and credit unions stated that the proposal would not meet its objectives related to privacy and security for various reasons. Some commenters suggested this would be the case because of a lack of regular examinations of third parties. Others took issue more generally with the obligation to make data available to third parties, which they said would open the door to fraud and security breaches of personally

identifiable data. Many data providers expressed concern that they would be obligated to ensure the data security of third parties.

Some data provider and third party commenters also raised concerns about the CFPB's legal authority for parts of the proposal. Some commenters also suggested that the CFPB consider consumer data sharing rules in other jurisdictions in drafting the final rule, but without clear consensus on what did or did not work in other jurisdictions.

Response to comments

The CFPB agrees with the general comments about implementing CFPA section 1033 to ensure data providers not only provide data access to consumers directly but also provide access for consumers' authorized third party representatives. As discussed in part III and part IV.C.2, this aspect of the rule is consistent with the plain language and objectives of section 1033 and the CFPA more broadly. In addition, the CFPB agrees that this aspect of the rule will increase opportunities for both depository and nondepository institutions to provide better products or services to consumers and enable consumers to manage their financial lives using data under the control or possession of data providers.

The CFPB also agrees with commenters that supported the general approach to third party access. As discussed in part IV.D, the third party access provisions of the final rule are designed to ensure, consistent with carrying out the objectives of CFPA section 1033, that consumers provide informed consent to third parties that access covered data pursuant to the final rule's framework, that consumers retain control over third parties' access, and that third parties act on behalf of consumers when collecting, using, and retaining covered data.

With respect to comments opposing the proposal, including due to concerns about the impact on competition, the final rule carries out Congress' objectives in CFPA section 1033(a)

and the mandate at CFPA section 1033(d) to prescribe standards to promote the development and use of standardized formats. As discussed further in part IV.D.1, Congress intended for consumers to be able to authorize third parties to access data under the statute on their behalf. Congress also directed the CFPB to prescribe standards to promote the development and use of standardized formats of information. The final rule carries out those objectives. For more discussion on the costs and benefits of the final rule, including impacts on competition, see parts VI and VII below.

The final rule will help ensure that markets for consumer financial products and services are competitive overall. Consumers will have even greater ability to take advantage of the many products or services already available, and data providers will have stronger incentives to enhance their products and services to retain their customers. The CFPB disagrees with arguments that consumers are not interested in third party data access, and notes that many consumers of institutions both large and small share data with third parties. But even where data providers already make data available voluntarily, the CFPB has determined the rulemaking is needed to address the challenges that have arisen in open banking, as discussed in the proposal. *See* 88 FR 74796, 74798-99 (Oct. 31, 2023).

As discussed further in part IV.A.3, the CFPB has determined it is appropriate to implement the product coverage of CFPA section 1033 in a staged manner. With respect to concerns about data provider incentives to block screen scraping, those incentives exist independent of the final rule. As safer forms of data access become functional, the CFPB expects that parties will move away from screen scraping. However, as discussed further in part IV.C.3, data providers must exercise caution when blocking screen scraping outside the rule's coverage.

With respect to the impact on the market for data aggregation, in the current market, and in the absence of implementing CFPA section 1033, open banking activity has already consolidated to data aggregators for the reasons discussed in the proposal. *See* 88 FR 74796, 74798-99 (Oct. 31, 2023). The impact of the rule on the value of intermediation arise from carrying out congressional intent to make consumer data more portable, including as a result of the interoperability objective inherent in CFPA section 1033(d)'s mandate to promote standardized formats. Additionally, whether an authorized third party relies on an aggregator is a business decision of the authorized third party. The final rule will reduce costs for authorized third parties generally, including the cost of using an aggregator, and should make it easier to access data directly from data providers over time, due to various aspects of the final rule including the requirements related to standardized formats, the prohibition on fees, and the rule's recognition of industry standard-setting as an important aspect of an effective and efficient open banking system.

With respect to concerns about competitive disadvantages for smaller data providers, the CFPB is not finalizing the rule with respect to depository institutions under the coverage threshold at § 1033.111(d) and is providing smaller data providers that are covered additional time to comply, as discussed in part IV.A.5. The rule also presents opportunities for small data providers to better compete by offering products and services to a wider range of consumers. One commenter expressed concern that excluding smaller data providers would disadvantage small data providers relative to large data providers that continued to have the obligation, but for which they would not offer developer interfaces. The CFPB disagrees with this premise and notes that many large data providers are already offering developer interfaces and that small data providers can participate in open banking voluntarily.

Some commenters expressed concern that the rule would force small data providers to rely on standards developed by large data providers with more resources. During the SBREFA process, the CFPB received feedback that standardization can reduce costs for small entities, including data providers and third parties.[32] Consistent with the mandate in CFPA section 1033(d), the final rule includes various provisions to promote the development and use of standardized data formats. Further, consensus standards (discussed in part IV.A.6 below) that can serve as indicia of compliance with various rule provisions, must be issued by a recognized standard setter that demonstrates balance, as discussed further in the Industry Standard-Setting Final Rule.

With respect to commenters that expressed concerns about obligations for authorized third parties, including the limitation on third party collection, use, and retention of covered data, the CFPB notes that those provisions ensure that consumers provide express informed consent to third parties that access covered data, that consumers retain control over third parties' access, and that third parties act on behalf of consumers when accessing covered data. The CFPB's responses to commenter concerns related to the third party authorization procedures and obligations are discussed below in part IV.D. Further, and as discussed in part IV.D.4, the CFPB disagrees with commenters' assertions that the rule would competitively disadvantage third parties relative to data providers. Data providers and third parties may use data that result from direct consumer relationships without adhering to the third party authorization procedures and obligations, and the final rule also does not treat covered data providers differently than other third parties when they act as authorized third parties themselves. With respect to comments about the competitiveness of the U.S. generally, the purpose of this rule is to ensure that third

[32] *See, e.g.*, SBREFA Panel Report at 28, 44.

parties are acting on behalf of consumers. With respect to comments about third party oversight and data security, see the discussion below in part IV.3, IV.5, IV.C.4-5, and IV.D.4.

2. Comments regarding the rulemaking process

The CFPB issued the proposed rule on its website on October 19, 2023, and published it in the *Federal Register* on October 31, 2023, with comments due by December 29, 2023. Some commenters asserted that the CFPB's comment period should have been longer. One commenter disagreed and suggested that requests to extend the comment period were pretextual efforts to delay implementation.

The Administrative Procedure Act does not specify a particular period of time for a public comment period,[33] and the comment period in this rulemaking was sufficient. This is illustrated by, among other things, the many detailed comments the CFPB received from stakeholders of all types, sizes, and viewpoints. Additionally, as noted above in part II, the CFPB has engaged in extensive public outreach since 2016 related to consumer-authorized data sharing, including through an RFI, an ANPR, and the SBREFA process. The CFPB also has taken various steps in response to the specific concerns raised with respect to the substantive provisions of the proposal. In particular, as discussed in part IV.A.4, the CFPB has determined to not finalize the rule with respect to small depository institution data providers.

3. Comments regarding liability among commercial entities

Comments received

Many commenters addressed the general topic of liability. A number of data provider commenters, academic researchers, and research institute commenters predicted that the final rule would increase the volume of sensitive financial data accessed by third parties, particularly

[33] *See* 5 U.S.C. 553(c).

sensitive information to initiate a payment (under proposed § 1033.211(c)), which they viewed as increasing the risk of unauthorized transactions or other harms arising from the compromise of a data provider's or third party's information systems, such as the risk of inaccurate data transmission. A number of data provider commenters noted that consumers might seek to hold data providers responsible for damages, or that data providers would face increased costs related to reimbursing consumers for a third party having fraudulently induced the consumer's authorization to access covered data. These commenters expressed concern that this would subject data providers to losses arising from liability and other compliance obligations, such as costs due to Regulation E and Z error investigations, preventing monetary losses to accounts, seeking reimbursement from third parties, and safety and soundness standards. Commenters also noted other laws, including State laws, related to "fraud," "negligence," "privacy," "identity theft," and "data security," but did not otherwise identify sources of liability. Several commenters also raised questions about the applicability of the FCRA, which are described separately below in part IV.4.

Many data provider commenters asserted that the proposal had not accounted for data providers' potential exposure to liability-related costs or ensured third parties had incentives to manage liability and otherwise demonstrate capacity to cover losses directly caused by third parties. Some of these commenters stated that the proposal had incorrectly assumed that liability could be allocated adequately through private agreements (including private payment network rules and bilateral contracts), the Electronic Fund Transfer Act (EFTA), 15 U.S.C. 1691 *et seq.*, the Truth in Lending Act (TILA), 15 U.S.C. 1601 *et seq.*, and their implementing regulations. Commenters generally suggested the CFPB address liability by mandating a comprehensive approach to assigning liability or safe harbors for data providers, clarifying the role of bilateral

data access agreements to allocate liability, or take other steps to reduce harms that might create liability risk. By contrast, a trade association representing third parties and a data aggregator stated that the liability allocation under EFTA and TILA, combined with the third party data security and privacy obligations under the proposal, would be adequate to address liability concerns, although these commenters also expressed concern about relying on bilateral contracts to allocate liability. One commenter stated that liability should flow with the data, but that data providers and authorized third parties should be permitted to allocate liability amongst themselves by contract.

In particular, a data provider commenter expressed criticisms of private network rules, stating that they do not give data providers sufficient ability to recoup losses among multiple third parties, some of which might not be financially viable or be downstream of the authorized third party and outside of contractual privity; they do not provide for a clear liability framework or sufficient fraud or data security protections for higher-risk "pay-by-bank" transactions; and they do not fully address the costs of error investigations or other customer service particularly where consumers expect data providers to make them whole following a data breach.

With respect to bilateral contracts, several data provider and third party commenters stated that they are costly to negotiate and enforce (including against third parties that might not be financially viable), would result in uneven liability allocations across the market, and would generally protect the interests of the largest data providers. Several third party commenters also expressed concern that they might include unnecessary terms based on an overbroad interpretation of third party risk management obligations or be used to deny access pretextually.

Data provider commenters also asserted that third party compliance with GLBA Safeguards Framework, as contemplated under the proposal, would be insufficient to protect

consumers or data providers from liability risk because third parties would lack incentives to manage their data security if they were not financially liable for their conduct, and because they are not subject to supervision. A consumer advocate commenter also stated that clear expectations for liability would provide third parties greater incentive to manage data security risks.

To address these concerns, a wide range of data provider commenters, a trade association representing third parties, an academic researcher, and a consumer advocate recommended that the regulatory text include a comprehensive liability-allocation provision for any losses arising from the third party's misuse of a consumer's payment credentials to conduct a fraudulent transaction, losses arising from the unauthorized access of payment credentials due to a data breach, or other losses arising from harms occurring from data in that party's possession. Several data provider commenters and academic researcher commenters noted that other open banking regimes around the world take a similar approach. One trade association noted that, while liability is traditionally determined based on which party has possession of the data, the rule does not indicate that this is the case. Other data provider commenters, including a number of credit union commenters, recommended that the final rule establish a "safe harbor" for data providers required to make data available under the final rule that protects the data provider from claims from consumers and third parties. Some commenters presented different versions of such an approach, such as by conditioning the absence of liability on whether the data provider had actual knowledge of the third party's data security risk, or the third party making representations about its data security practices, or on the third party's possession of a certification or credential.

While some data provider and third party commenters expressed concern with reliance on bilateral data access agreements to allocate liability, some of these data provider commenters

stated that they could be used to address liability concerns. Several data provider commenters recommended that the final rule address liability by clarifying that data providers are not precluded from exercising discretion to comply with prudential safety and soundness obligations, including third party risk management expectations. Several of these commenters recommended that data providers be permitted to deny third parties, including data aggregators, access to a developer interface if they did not accept contractual terms related to liability, such as indemnification and insurance obligations. Several data provider commenters and related trade associations recommended that third parties be required to have or certify that they have adequate capital or insurance to cover losses. However, a data aggregator commenter stated that the rule should affirm the adequacy of the existing liability framework under EFTA and Regulation E and TILA and Regulation Z to help limit liability disputes during negotiations of bilateral data access agreements. Comments related to the role of such agreements in managing third party risk are discussed in greater detail in part IV.C.4 below.

Data provider commenters also recommended that the rule address liability by subjecting third parties to additional data security obligations, such as the FFIEC information security handbook appliable to depository institutions (discussed further below in part IV.D) or CFPB supervision. A research institute commenter also supported clarifying the CFPB's intent to supervise third parties as a way to reduce concerns related to liability.

A data provider commenter requested that the final rule clarify whether the data provider has any liability in the context of specific provisions of the proposal: (1) if a third party collects more information than is necessary to offer a specific product or service; and (2) if a data breach occurs because an authorized third party does not delete data after a consumer revokes its authorization or does not timely communicate the revocation to a data aggregator.

Response to comments

The CFPB has determined it would not be appropriate for this rule to impose a comprehensive approach to assigning liability among commercial entities or safe harbors from the requirements of EFTA and Regulation E or TILA and Regulation Z. The ability of payees to initiate electronic payments has existed for decades and the Regulation E concerns raised by commenters are not specific to CFPA section 1033. Although this rule facilitates sharing of payment initiation information with third parties so that they can initiate electronic payments, the rule does not require account write access or otherwise require payment initiation. Applicable payment authorization requirements continue to separately apply. As noted in the proposal, consumers have a statutory right under EFTA to resolve errors through their financial institution, while private network rules, contracts, and other laws address which payment market participant is ultimately liable for unauthorized transfers and other payment errors. As discussed further below, the U.S. payment system allows non-bank payees to initiate payments through their depository institution, and those partner depository institutions also bear responsibility for who is allowed to access the payment networks.

The CFPB is aware that it is common for non-bank payees, such as utility companies, charities, non-bank lenders, community organizations, and other billers, to initiate payments through their depository institution. The payee's depository institution, referred to as an originating depository financial institution in the context of ACH payments, is responsible for ensuring that any payments it initiates on the payee's behalf are correct and authorized, as they are subject to private network rules and safety and soundness requirements related to risk

management.[34] Data providers that are Regulation E financial institutions will continue to have error resolution obligations for transfers initiated using payment information shared under this rule, just as they do today when a consumer shares information with a payee or a consumer's payment credentials are compromised, and can seek reimbursement from an originating depository financial institution according to private network rules, contracts, and commercial law. For example, although a consumer's financial institution is required to reimburse the consumer for an unauthorized transfer under Regulation E, ACH private network rules generally dictate that the receiving depository financial institution is entitled to reimbursement from the originating depository financial institution that initiated the unauthorized payment. Similarly, data providers that are Regulation Z credit card issuers will continue to have error resolution obligations under TILA. Commenters did not identify a plausible method through which the proposal would increase the risk of credit card fraud. The final rule does not require data providers to make available credit card payment information. For both Regulation E accounts and Regulation Z credit cards, because the final rule only requires data providers to share information and does not require that they allow third parties to initiate payments using that information, any costs arising from error investigations and the recoupment of losses by data

[34] *See, e.g.*, OCC Bulletin 2006-39, *Automated Clearing House Activities: Risk Management Guidance* (Sept. 1, 2006), https://www.occ.gov/news-issuances/bulletins/2006/bulletin-2006-39.html; NACHA Operating Rules Section 2.2: Warranties and Liabilities of Originating Depository Financial Institutions; NACHA Operating Rules Subsection 2.2.3 Liability for Breach of Warranty ("Each ODFI breaching any of the preceding warranties shall indemnify each RDFI, ACH Operator, and Association from and against any and all claim, demand, loss, liability, or expense, including attorney's fees and costs, that result directly or indirectly from the breach of warranty or the debiting or crediting of the entry to the Receiver's account. This indemnity includes, without limitation, any claim, demand, loss, liability, or expense based on the ground that the debiting of an entry to an account resulted, either directly or indirectly, in the return of one or more items or entries of the Receiver due to insufficient funds. This indemnity also includes, in the case of a Consumer Account, without limitation, any claim, demand, loss, liability, or expense based on the ground that the failure of the ODFI to comply with any provision of these rules resulted, either directly or indirectly, in the violation by an RDFI of the Federal Electronic Fund Transfer Act or Federal Reserve Board Regulation E.").

providers are a function of how private network rules operate. The final rule does not impinge on such private arrangements.

Commenters suggested that consumer-authorized data sharing may create risks to consumers and financial costs to financial institutions arising from an increased risk of unauthorized transactions and other errors, especially when data access relies on screen scraping. In implementing CFPA section 1033, the CFPB is finalizing a variety of measures to mitigate unauthorized transfer and privacy risks to data providers and consumers, including allowing data providers to share TANs; not allowing data providers to rely on credential-based screen scraping to satisfy their obligations under CFPA section 1033; clarifying that data providers can engage in reasonable risk management activities; implementing authorization procedures for third parties that would require they commit to data access, use, and retention limitations; implementing policies and procedures regarding data accuracy; and requiring compliance with the GLBA Safeguards Framework. These provisions are intended to drive market adoption of safer data sharing practices. With respect to commenters' suggestions to reduce costs associated with liability through data access agreements or other conditions for third parties attempting to access consumer data, see parts IV.C.4 and IV.D.4. With respect to the suggestion that authorized third parties certify to consumers as to capital adequacy or insurance, see part IV.D.1 for discussion of comments.

Finally, the CFPB does not believe it would be appropriate to attempt to establish a comprehensive approach to addressing liability (including through safe harbors) for laws it does not administer, such as State laws dealing with data security, privacy, identity theft, negligence, and fraud. The extent of data providers' liability for failure to comply with their obligations under this final rule is provided for under the CFPA.

The CFPB also notes that commenters did not provide legal analysis or factual evidence about the likelihood that data providers would actually incur legal liability under these laws when consumers request, or Federal law requires, they make data available to a third party that subsequently misuses or mishandles the data. While some commenters stated that consumers would be likely to seek to recoup from the data provider losses arising from third party conduct, it is not clear to what extent that is likely to occur when losses arise from a third party to which the consumer requested the data provider make information available. To the contrary, a trade association commenter indicated that liability typically resides with the party that experiences a data breach. Nor did commenters provide evidence of the extent to which data providers actually defend against claims of such liability, despite data providers' long-standing practice of consumer-authorized third party data sharing. To the extent there are complex factual or legal questions about a data provider's liability for directly contributing to consumer harm, commenters did not identify particular scenarios, and the CFPB does not believe it would be appropriate to make statements about a data provider's liability in this final rule. As an additional and independent reason, commenters did not identify the legal authority the CFPB could rely on to modify laws it does not administer.

4. Comments regarding potential overlaps with other consumer financial laws and CFPB rulemaking activity

Electronic Fund Transfer Act and Regulation E

Comments

In addition to the liability comments discussed above, some data provider commenters specifically commented on the applicability of EFTA and Regulation E. Some data provider commenters asked the CFPB to apply Regulation E error investigation requirements to all third

parties. A few data provider commenters stated that the CFPB should clarify that data aggregators are Regulation E service providers, asserting that the data aggregator is in the best position to control for risks related to the transactions it permits a consumer to conduct through its system. A trade association representing data providers asked the CFPB to clarify that a data access agreement between an aggregator and data provider is an "agreement" for purposes of the Regulation E service provider provision. A data provider commenter asked the CFPB to clarify that, if a third party is a Regulation E financial institution, such as a digital wallet provider that obtains permissioned data access under CFPA section 1033, it would have error resolution responsibilities for payments initiated using data obtained from the developer interface and that such digital wallet providers should be required to provide their contact information to consumers.

Response to comments

The CFPB has determined that it is not appropriate or practical to deny consumers their statutory right to resolve errors through their financial institution and this final rule does not change such rights under EFTA and Regulation E. The Regulation E definition of financial institution means a bank, savings association, credit union, or any other person that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide electronic fund transfer services.[35] The CFPB declines to expand the scope of the Regulation E service provider provision to data aggregators, because doing so would limit consumers' ability to resolve errors and unauthorized transactions through their account-holding financial institution. Whether a given entity is a service provider for a given electronic fund transfer will depend on the relationship between the entities involved in making

[35] 12 CFR 1005.2(i).

that individual transfer, not whether the payee used payment credentials shared under this final rule to initiate the payment. Negating a consumer's statutory right to go to their financial institution to resolve errors also would result in an illogical and harmful error resolution regime. From the consumer's perspective, they may not know whether an error is related to data that was shared under CFPA section 1033. The CFPB is aware that some financial institutions attempted to have consumers enter into agreements to waive EFTA rights in situations where they shared account credentials or other information with a third party, even though such agreements violated the EFTA anti-waiver provision in 15 U.S.C. 1693l.[36] It was unclear at the time how exactly the depository institutions intended to enforce this waiver language. One concern was that it would be used to deny all Regulation E error resolutions rights to consumers who had shared any information with a data aggregator, even if the financial institution did not know whether the error was related to that shared information. It also would be burdensome and likely infeasible for the consumer to sort out when they should go to their financial institution for help versus a third party versus another entity for a transaction that they do not recognize.

Data providers and third parties that are Regulation E financial institutions—including digital wallet providers, person-to-person payment providers, entities that refer to themselves as neobanks, and traditional depository institutions—have and will continue to have error resolution obligations in the event of a data breach where stolen account or ACH credentials are used to initiate an unauthorized transfer from a consumer's account and the consumer provides proper notice. These error resolution obligations include requirements on the financial institution to provide consumers with the financial institution's contact information.

[36] *See* Consumer Fin. Prot. Bureau, *Regulation E FAQs, Error Resolution: Unauthorized EFTs #8*, https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/ (last updated June 4, 2021).

Fair Credit Reporting Act and Regulation V

The proposal noted that a third party engaged in data aggregation activities could be a consumer reporting agency under the FCRA if it met the elements of the FCRA's definition of "consumer reporting agency."

Comments

Some commenters addressed the applicability of the FCRA. Many data providers and data provider trade association commenters stated that the final rule should provide that data providers are not furnishers when they provide data pursuant to consumer authorization. These commenters asserted that the compliance burden of being a furnisher is significant and could overwhelm smaller financial institutions. They also argued that, unlike traditional furnishing, data providers sharing data under CFPA section 1033 are simply facilitating consumers' requests to access their data.

Other commenters, primarily data aggregators, stated that data aggregators should not be considered consumer reporting agencies when they transfer data pursuant to consumer authorization. These commenters argued that consumer-authorized data sharing is different from the provision of consumer reports because consumers have control over the sharing of their data, because data aggregators act as mere conduits for transmission of the data, and because consumers have direct relationships with data aggregators. One data aggregator commenter predicted that if data aggregators could be consumer reporting agencies, then data providers that are FCRA-covered furnishers would deny access unless the aggregators agreed to data access agreements with terms related to indemnification for FCRA liability. A third party trade association commenter contended that data providers that are FCRA-covered furnishers could deny access to data aggregators in the absence of a data access agreement. Other commenters

stated that treating data aggregators as consumer reporting agencies would result in unintended consequences. For example, a third party trade association commenter asserted that compliance with the FCRA could require data aggregators to access and retain more data than they do currently. And a data aggregator commenter stated that consumers might be confused if they attempt to correct the accuracy of any information transferred by a data aggregator, because data aggregators do not hold the underlying data; therefore, the data held by the data aggregator may differ from the versions held by the data provider and other third parties.

Some commenters requested that the final rule exclude FCRA-covered entities and data from the rule's coverage. Several consumer reporting agency commenters and a consumer reporting agency trade association commenter asserted that consumer reporting agencies should be excluded from coverage because they are already subject to extensive regulation under the FCRA. A data aggregator commenter suggested that the CFPB rely on existing authorities and not impose new regulations on the collection, use, and retention of covered data where such collection, use, and retention may be addressed by other laws, such as the FCRA. And a consumer reporting agency commenter stated that consumer reports should be excluded from the definition of "covered data" because otherwise the limited purposes that authorize consumer reporting agencies to share consumer reports might conflict with the purposes for which consumers might authorize sharing of their covered data. The consumer reporting agency trade association commenter stated that the proposed limitations on use and retention of covered data might complicate FCRA compliance by entities offering products that rely on indefinite consumer authorization, including products that allow consumers to self-report rental and utility payment information to their credit file to enhance their credit histories. Data aggregator commenters and a third party trade association commenter claimed that the FCRA's framework

is complex and confusing when applied in the context of consumer-authorized data access. And a data aggregator commenter asserted that the proposed rule's consumer protections would be more appropriate for consumer-authorized data access than FCRA requirements.

Several commenters raised questions about the intersection of the final rule and the FCRA, including the extent of overlap, duplication, or conflict between the final rule and the FCRA. These commenters asked for clarification on various specific questions, including: which activities would make a data provider an FCRA-covered furnisher; which use limitation standard applies if consumer-authorized data are subject to both the final rule and the FCRA; which activities would make a data aggregator a consumer reporting agency; whether data aggregators that are consumer reporting agencies would have to provide consumer reports to consumers at their request; how data aggregators that are consumer reporting agencies would comply with their FCRA dispute obligations if data providers are not FCRA-covered furnishers; how data aggregators that are consumer reporting agencies could maintain accurate consumer reports given the proposed limits on retention; which uses of covered data constitute permissible purposes under the FCRA; whether third parties can be both data aggregators under the final rule and consumer reporting agencies under the FCRA; whether financial institutions may combine disclosures and consent forms required by the final rule and the FCRA; whether specialty consumer reporting agencies may collect and retain consumer-authorized transaction data to comply with the FCRA; and whether information from de-identified consumer reports used for research purposes could also be covered data subject to the proposed restrictions on secondary use.

Finally, some commenters stated that the CFPB should coordinate the FCRA and Personal Financial Data Rights rulemakings.[37] A bank trade association and credit union trade association stated that until one of these rules had been finalized, they could not fully understand the impacts of one rule on the other. A data provider/third party trade association commenter suggested pausing the FCRA rulemaking until the Personal Financial Data Rights rulemaking is finalized to fully understand each rule's impact. A consumer reporting agency commenter, an industry trade association commenter, and a financial holding company commenter requested that the Personal Financial Data Rights final rule be issued before the FCRA proposed rule. The industry trade association commenter and financial holding company commenter asserted that concurrent rulemaking adversely impacts the public's ability to meaningfully comment on each proposal. A bank trade association commenter recommended postponing compliance with this final rule until after an FCRA rule is finalized, while a data aggregator commenter asked the CFPB to wait until after this rule is finalized to address the applicability of the FCRA to data aggregators. And a research institute commenter suggested that certain definitions, such as those relating to data aggregators and FCRA-covered furnishers, be harmonized between the final rule and the FCRA rulemaking.

Response to comments

As an initial matter, the CFPB has determined that this final rule does not affect a person's obligations or duties under the FCRA. The final rule does not alter the types of data, parties, or permissible purposes covered by the FCRA. Because the final rule does not change

[37] The CFPB assumes commenters were contemplating an FCRA rulemaking with a scope similar to what was described in the CFPB's FCRA 2023 SBREFA Outline, which included proposals under consideration related to data broker activities and medical debt information. *See* Consumer Fin. Prot. Bureau, *Small Business Advisory Review Panel for Consumer Reporting Rulemaking Outline of Proposals and Alternatives Under Consideration* (Sept. 15, 2023), https://files.consumerfinance.gov/f/documents/cfpb_consumer-reporting-rule-sbrefa_outline-of-proposals.pdf.

substantive requirements under the FCRA or Regulation V, the commenters that raised questions about the intersection of the FCRA with CFPA section 1033 and how to comply with FCRA obligations and duties must look to the FCRA and Regulation V to determine how to comply with a particular FCRA requirement. For example, whether a third party, such as a data aggregator, is a consumer reporting agency under the FCRA depends on whether the third party falls within the definition of "consumer reporting agency" in the FCRA.[38] Similarly, whether a certain use of covered data constitutes a permissible purpose is determined by looking to the FCRA.[39] This is true with respect to any question about what a person subject to this final rule must do to comply with the FCRA and Regulation V.

The CFPB also has determined that the requirements of this final rule are not inconsistent with the FCRA or Regulation V. Some commenters noted that certain uses of data might be permitted by the FCRA but not authorized by the Personal Financial Data Rights rule as proposed. Compliance with this final rule does not, however, require a person to violate the FCRA or Regulation V. Therefore, a person that is subject to this final rule and the FCRA/ Regulation V must comply with both. This is no different than for any person who is subject to several overlapping laws and regulations. For example, a third party may have to contemporaneously provide disclosures relating to Regulation E accounts, Regulation Z credit cards, and the GLBA and Regulation P. When applicable, a third party subject to all these laws must satisfy their respective requirements. Complying with CFPA section 1033 and the final rule is no different. Thus, it is unnecessary to exclude certain parties, such as consumer reporting agencies, or FCRA-covered uses from the rule's coverage.

[38] *See* 15 U.S.C. 1681a(f) (defining consumer reporting agency).

[39] *See* 15 U.S.C. 1681b (identifying permissible purposes).

The CFPB also received comments about whether data providers are furnishers under the FCRA. The CFPB would not consider data providers under this final rule to be furnishers solely by virtue of permitting data access pursuant to an authorization that is consistent with the final rule. This is the case even assuming data are provided to a data aggregator that qualifies as a consumer reporting agency. In these unique circumstances, the consumer, and not the data provider, would be the party that is furnishing data to the consumer reporting agency. This is the case because of a particular combination of circumstances, including that the data are only shared with the aggregator after the data provider is asked to do so by the consumer; the data are shared pursuant to a written authorization designed to ensure that the consumer has meaningful control of the uses of the specific data that are shared; the data are further protected by use restrictions to ensure they continue to be used for the benefit of the consumer; and the data provider is not exercising its own agency or control or benefiting from the arrangement, but rather is simply facilitating the consumer's decision to furnish.[40]

The CFPB received comments seeking clarification about whether data aggregators are consumer reporting agencies under the FCRA. However, this final rule does not cause data aggregators to incur legal liability under the FCRA that they would not otherwise assume through their ordinary operations. Addressing this topic is not necessary to finalize this rulemaking because whether a data aggregator is a consumer reporting agency under the FCRA requires a fact-specific inquiry of considerations beyond the scope of this final rule. Data aggregators may engage in a variety of activities and have multiple business models, and whether a data aggregator is a consumer reporting agency will depend on the satisfaction of all

[40] *See, e.g.*, 12 CFR 1022.41(c)(3) (Under the Furnisher Rule in Regulation V, when the consumer furnishes information to a CRA about themselves, the consumer is not considered a "furnisher.").

components of the statutory definition in the FCRA—a determination not affected by this final rule.

The CFPB disagrees that the sequencing of the Personal Financial Data Rights and FCRA rulemakings adversely impacted the public's ability to comment on the Personal Financial Data Rights proposed rule. After issuing the Personal Financial Data Rights proposed rule, the CFPB published a proposed rule regarding medical information under the FCRA. *See* 89 FR 51682 (June 18, 2024) (Medical Debt Proposed Rule). The Medical Debt Proposed Rule would remove a regulatory exception in Regulation V from the limitation in the FCRA on creditors obtaining or using information on medical debts for credit eligibility determinations and would limit the circumstances under which consumer reporting agencies are permitted to furnish consumer reports containing medical debt information to creditors when making credit eligibility determinations. The CFPB is also engaged in a rulemaking focused on data broker activities (Data Broker Rulemaking).

With respect to the sequencing of the Personal Financial Data Rights and the Medical Debt and Data Broker rulemakings, the fact that this final rule does not change what a person would need to do to comply with its existing obligations under the FCRA means that completing the Medical Debt and Data Broker rulemakings is not necessary to finalize this rulemaking. The CFPB will consider feedback received in the course of the Medical Debt and Data Broker rulemakings, evaluate the further steps it may take in those rulemakings, and will respond to comments as appropriate.

The CFPB acknowledges that the potential applicability of the FCRA to uses of covered data under the final rule presents operational complexity, and the CFPB is taking steps to coordinate the final rule with the ongoing FCRA rulemakings. As described in part IV.A.5, the

CFPB is substantially revising the compliance deadlines for data providers under the final rule. The CFPB has determined that the extension of the compliance deadlines strikes the appropriate balance between carrying out the objectives of the statute while also providing an entity covered by the final rule with more time to work through these operational challenges and understand the entity's compliance obligations under the final rule in light of the FCRA.

Gramm-Leach-Bliley Act and Regulation P

A few commenters addressed the general applicability of the GLBA and Regulation P, 12 CFR part 1016. Several commenters asked for clarity about how financial institutions should comply when data are subject to both the GLBA and the Personal Financial Data Rights rule. For example, a bank commenter and a bank trade association commenter asked which use limitation standard would apply. A third party commenter suggested that the CFPB rely on existing authorities and not impose new regulations on the collection, use, and retention of covered data where the collection, use, and retention of the data may be addressed by other laws, including the GLBA. A research institute commenter asserted that consumers might be confused if they received multiple disclosures.

Response to comments

The CFPB has determined that the final rule does not affect a person's obligations or duties under the GLBA. In addition, the CFPB has determined that the final rule is not inconsistent with the GLBA or Regulation P. As with the FCRA, some commenters sought clarification about how a person would comply when data are subject to the GLBA and CFPA section 1033, including whether the limitations on collection, use, and retention of data under the final rule would apply where such limitations are not imposed under the GLBA and Regulation P. While the GLBA and Regulation P may permit some uses of information that may

not be permitted under the final rule, compliance with the final rule does not require a person to violate the GLBA or Regulation P. Moreover, the CFPB expects that a person covered by the final rule is experienced with managing the respective requirements of applicable State and Federal laws, including the implementation of overlapping disclosure requirements.

Other commenters raised broader issues. For example, a data aggregator commenter suggested that the CFPB should encourage Congress to amend GLBA or pass a Federal data privacy law. This commenter also suggested that the CFPB undertake a GLBA rulemaking. These comments are outside the scope of this rulemaking.

The CFPB declines to rely on existing legal frameworks, including the GLBA and Regulation P, to regulate consumer privacy. The purposes and objectives of CFPA section 1033, which are described in part III.A, differ in certain respects from the purposes and objectives of other laws (such as the GLBA). The requirements set forth in the final rule are better suited to the open banking context, and could not be substituted by applying existing authorities to consumer-authorized access of covered data.

Comments addressing the GLBA in relation to a specific proposed provision, such as comments recommending the final rule adopt Regulation P's privacy protections for third parties, are addressed in part IV.C and D.4.

CFPA Section 1034(c)

Section 1034(c) of the CFPA generally requires large financial institutions to comply with consumer requests for information concerning their accounts in a timely manner, subject to certain statutory exceptions.[41] In October 2023, prior to the proposal, the CFPB issued an

[41] Specifically, CFPA section 1034(c) applies to insured depository institutions (including credit unions) that offer or provide consumer financial products or services and that have total assets of more than $10 billion, as well as their affiliates.

advisory opinion on CFPA section 1034(c) that interprets this provision for the purpose of highlighting the obligations it imposes upon large financial institutions.[42] One commenter asked the CFPB to clarify the extent to which the scope of data covered by CFPA section 1033 and by the CFPA section 1034(c) advisory opinion overlap, and how that may impact obligations for data providers.

CFPA sections 1033(b) and 1034(c)(2) both generally apply to "information in the control or possession" of a covered person "concerning the consumer financial product or service that the consumer obtained from such covered person." However, the statutes differ in several respects, including the types of covered persons subject to, the exceptions to information covered by, and the form in which information must be provided pursuant to the statutes.

The statutes impose separate obligations on large depository institutions (including credit unions), and how the statutes impact institutions' obligations will depend on the facts.[43] As noted in the advisory opinion:

> [S]ection 1033 governs consumer authorized third-party access to data made available in electronic form in connection with third-party provision of other products or services—including for example, the provision of a potentially competing account offering. This is why, for example, section 1033 is limited to data available in the normal course, and why section 1033 requires data to be 'made available . . . in electronic form.'[44]

See also part IV.C regarding a comparison between CFPA sections 1034(c) and 1033 with respect to the final rule's prohibition on fees for data access.

---

[42] Consumer Fin. Prot. Bureau, *Consumer Information Requests to Large Banks and Credit Unions*, 88 FR 71279 (Oct. 16, 2023).

[43] As noted in the advisory opinion, the CFPB does not interpret section 1034(c) to preempt or otherwise supersede the requirements of other Federal or State laws and regulations designed to protect privacy and data security, including, for example, any restrictions that may be imposed in the CFPB's upcoming rule implementing section 1033. *See* 88 FR 71279, 71279 n.27 (Oct. 16, 2023).

[44] *See id.* at 71279 n.23.

5. Other comments

A number of commenters sought information on how the CFPB will conduct oversight of third parties. Commenters stated that many authorized third parties are outside the CFPB's enforcement or supervisory jurisdiction, and asserted that data aggregators pose relatively greater risks to consumers than authorized third parties. Some commenters also asked whether the CFPB would consider complaints from industry participants when setting supervision and enforcement priorities, and asked that the CFPB encourage consumers to submit complaints to its consumer complaint program.[45] Several commenters sought information on how the CFPB would provide guidance after the final rule is issued. In addition, a consumer advocate recommended that the CFPB engage in a consumer education campaign to inform consumers of their rights under the rule. The commenter explained that improved consumer understanding of consumer-authorized data sharing would increase consumer confidence in sharing data and protect them from bad actors.

SBA Advocacy requested that the CFPB determine whether the final rule is necessary in light of current State law (citing the California Consumer Privacy Act as an example) and whether the final rule conflicts with State laws. Other commenters questioned whether the CFPB had taken proper account of international open banking regimes in developing the proposal.

With respect to questions about how the CFPB intends to enforce and supervise for the requirements that apply to third parties, § 1001.2(b) of the final rule provides additional assurance that financial data processing by third parties, among others, is subject to the CFPA. This includes enforcement and, where appropriate, supervision, by the CFPB. In addition, the

[45] *See generally* Consumer Fin. Prot. Bureau, *Submit a complaint about a financial product or service*, https://www.consumerfinance.gov/complaint/ (last visited Oct. 17, 2024).

CFPB and FTC coordinate law enforcement activities regarding the offering or provision of consumer financial products and services by covered persons within the FTC's jurisdiction under the FTC Act, including conducting joint investigations where appropriate, to minimize duplication of efforts and burden on FTC-covered industry participants. This may include coordination on enforcement activities regarding the CFPA prohibition on unfair, deceptive, or abusive acts or practices and the FTC Safeguards Rule. The CFPB also coordinates with State attorneys general and State regulators. With respect to questions about the role of consumer complaints in establishing supervision and enforcement priorities, the CFPB prioritizes supervisory and enforcement activity on the basis of risk, taking into account, among other factors, the size of each entity, the volume of its transactions involving consumer financial products or services, the size and risk presented by the markets in which it is a participant, the extent of relevant State oversight, and any field and market information that the CFPB has on the entity. Such field and market information can include, for example, information from complaints and any other information the CFPB has about risks to consumers and to markets posed by a particular entity. In response to comments advocating for CFPB supervision of third parties, including data aggregators, the CFPB's supervisory authority is defined by the CFPA. The CFPB agrees that supervision of data aggregators is important. Supervisory examinations over one or more data aggregators, including larger participants in the consumer reporting market, are scheduled or ongoing,[46] and the CFPB will continue to engage in this supervision as necessary.

With respect to guidance after the final rule is issued, the CFPB plans to make available a range of resources to assist with effective implementation of the rule, including a small entity compliance guide. The CFPB also has a regulatory support program that can provide assistance.

[46] *See* Supervisory Highlights, Issue 30, Summer 2023, 88 FR 52131, 52142 (Aug. 7, 2023).

With respect to comments about improving consumer awareness of their rights under this rule, the CFPB notes that the consumer protections in this rule are intended to ensure that consumers can access their own data and can authorize access by third parties that are acting on their behalf. For more discussion of consumer awareness of third party access, see part IV.D below. The CFPB intends to further consider how to increase consumer awareness of and confidence in authorized third party data access.

The CFPB has considered State law and international legal frameworks to inform the final rule's approach to data providers' obligations to make data available upon request and third parties' obligations to act on behalf of consumers in order to access such data. Several States impose obligations on businesses to make information available to consumers in a portable, structured format, where technologically feasible.[47] Several States also impose privacy obligations on businesses. However, these State laws differ in terms of their scope and substantive requirements. In addition, a number of States include exemptions for businesses or data covered by certain Federal consumer financial laws, like the GLBA.[48] The CFPB believes it is appropriate to carry out congressional intent to issue Federal regulations pursuant to CFPA section 1033, including the interoperability objectives of CFPA section 1033(d), by issuing requirements applicable nationwide to promote safe, secure, reliable, and competitive data access. The CFPB is not aware of conflicts between State law and the final rule. See parts VI and VII for further discussion of the impacts of State law.

As part of this rulemaking, the CFPB has considered international open banking models, as discussed in the proposed rule and further below. The CFPB's authority and policy approach

[47] *See, e.g.*, Cal. Consumer Privacy Act of 2018 section 1798.130(a)(3)(B)(i)-(iii).

[48] *See, e.g.*, *id.* section 1798.145(e). *See also* SBREFA Outline at 46 n.50.

in this final rule are not identical to those of other jurisdictions. In particular, as discussed in part IV.3, IV.C.2, and elsewhere in part IV, the final rule does not require data providers to initiate payments, unlike some other open banking regimes. The final rule instead implements CFPA section 1033 with respect to a data provider's obligation to make available covered data to consumers and third parties authorized to access such data on their behalf. The CFPB has taken account of the experience of international jurisdictions in developing the final rule generally and as discussed in part IV.C.2 with respect to the prohibition on fees for third party access, part IV.C.3 with respect to commercially reasonable performance standards, and the final rule's approach to screen scraping, as discussed in part IV.D.1. The CFPB believes any differences between the approach of this final rule and those of other jurisdictions are appropriate in light of the particular market and regulatory frameworks applicable to the U.S. See parts VI and VII for further discussion of international jurisdictions.

A. Subpart A—General

1. Overview

Subpart A of the final rule establishes the coverage and terminology necessary to implement CFPA section 1033 for this rule, beginning with § 1033.101, which describes the authority, purpose, and organization of the regulation in part 1033. Subpart A defines the coverage of the final rule, sets forth tiered compliance dates, defines terms appearing throughout the regulatory text, and, as finalized in the Industry Standard-Setting Final Rule, sets forth criteria for recognized standard setters.

2. Authority, purpose, and organization (§ 1033.101)

In the proposed rule, the CFPB proposed § 1033.101(a) to describe the CFPB's legal authority to issue the rule for the purposes described in proposed § 1033.101(b). Proposed

§ 1033.101(c) described the organization of the proposed rule within part 1033. The Industry Standard-Setting Final Rule finalized the language in proposed § 1033.101(a) and a more limited version of proposed § 1033.101(b) and (c), to reflect the limited purpose and organization of the Industry Standard-Setting Final Rule. The CFPB did not receive comment on the proposed rule's proposed language in § 1033.101.

In this final rule, the CFPB is not making changes to the legal authority language in § 1033.101(a) that was finalized by the Industry Standard-Setting Final Rule. The CFPB is amending the language finalized by the Industry Standard-Setting Final Rule at § 1033.101(b) and (c), as originally proposed by the proposed rule, to reflect the purpose and organization of this final rule. Final § 1033.101(c) also refers to the appendix containing standard-setter recognition procedures that was finalized as part of the Industry Standard-Setting Final Rule. Other than with respect to § 1033.101, the final rule published in this *Federal Register* document does not amend any of the provisions of the Industry Standard-Setting Final Rule. The regulatory text published in this *Federal Register* document restates the regulatory text finalized in the Industry Standard-Setting Final Rule (other than with respect to § 1033.101) for clarity and ease of reading.

3. Coverage of data providers (§ 1033.111(a) through (c))

Proposal

Section 1033(a) applies to "covered persons," as defined in the CFPA. In the proposal, the CFPB explained its intent to implement the broad coverage of CFPA section 1033 through this and supplemental rulemaking. For this first rule to implement coverage and other substantive provisions of CFPA section 1033(a), the CFPB proposed to define a subset of covered persons that would be required to make data available with respect to certain consumer financial products

or services: Regulation E asset accounts, Regulation Z credit cards, and products or services that facilitate payments from a Regulation E account or a Regulation Z credit card. The CFPB explained that the last of these categories would clarify that the proposed rule would cover all consumer-facing entities involved in facilitating Regulation E account and Regulation Z credit card transactions.

In the proposed rule, the CFPB discussed how payment data from these products and services support common beneficial consumer use cases today, including transaction-based underwriting and payment initiation. Specifically, the CFPB proposed in § 1033.111(b) to define covered consumer financial product or service to mean (1) a Regulation E account, a defined term that would have the same meaning as defined in 12 CFR 1005.2(b); (2) a Regulation Z credit card, a defined term that would have the same meaning as defined in 12 CFR 1026.2(a)(15)(i); and (3) the facilitation of payments from a Regulation E account or Regulation Z credit card. The CFPB proposed in § 1033.111(c) to define data provider to mean a covered person, as defined in 12 U.S.C. 5481(6), that is (1) a Regulation E financial institution, as defined in 12 CFR 1005.2(i); (2) a Regulation Z card issuer, as defined in 12 CFR 1026.2(a)(7); or (3) any other person that controls or possesses information concerning a covered consumer financial product or service the consumer obtained from that person. In example 1 to § 1033.111(c), the CFPB proposed to provide an example that a digital wallet provider is a data provider. The CFPB requested comment on the proposed definitions.

The proposed rule also explained that the CFPB was considering adding EBT-related data to the final rule, or reaching EBT cards in a subsequent rulemaking. State and local administered needs-tested benefits are exempt from EFTA coverage by statute. When distributed electronically, needs-based benefits established under State or local law or administered by a

State or local agency are primarily issued to consumers via EBT cards. EBT-related data are mainly accessed directly by the consumer through private entities that have contracted with State or local governments that administer programs for Federal government agencies. The CFPB requested comment on whether the most appropriate way to solve issues related to EBT data accessed directly by the consumer is through section 1033 of the CFPA, and whether it should do so as part of this first rulemaking related to payments data or a subsequent rule under CFPA section 1033. The CFPB also requested comment on third party practices related to consumer-authorized EBT data, and the benefits and drawbacks of enabling third party access to EBT-related data, including with respect to data security.

Comments

Many commenters, including third parties and consumer advocates, stated that the proposed coverage was too narrow. Advocated additions included all covered persons and financial products and services under the CFPA, all Regulation Z creditors (such as mortgage, auto, and payday lenders), payroll providers, holders of tax records, electronic bill presentment providers, investment products, retirement accounts, and small business lenders. Some third party commenters asserted that data providers will otherwise restrict or fail to offer access to these data. One bank data provider commenter stated that the narrow scope of coverage could cause consumer confusion. A non-bank data provider that also acts as a third party stated that coverage should be broader because much or all of the covered data are already made available by banks today.

Conversely, many data provider commenters requested narrower coverage, and that the CFPB clarify the rule's applicability, particularly with regard to pass-through payments and payment facilitation providers. Some commenters asked for specific exclusions for products or

entities that they asserted are excluded from the CFPB's authority under the CFPA, such as corporate credit cards and merchants. Several third party and trade association commenters asked the CFPB to clarify that the rule does not cover other entities that initiate payments on the payee's behalf, such as embedded payment service providers that provide payment processing services exclusively for merchants, third party marketplaces operated prominently in the name of their affiliate company, and loan servicers. One non-bank data provider that also acts as a third party asked the CFPB to exclude online marketplaces and ride sharing apps. Two data provider trade associations asked the CFPB to exclude inactive or closed accounts.

Two trade associations commenting on the CFPB's TILA interpretive rule regarding credit products marketed as BNPL,[49] along with a provider of BNPL products, stated that the Personal Financial Data Rights rule should not apply to BNPL providers because they lacked notice that such providers are card issuers under Regulation Z and that the proposal did not adequately account for the impact on BNPL providers. A third party trade association supported coverage of BNPL providers as data providers, explaining in a comment on the CFPB's TILA interpretative rule that it supports the consumer right to share their balance and transaction information for any and all of their credit accounts. A few bank data provider trade associations commenting on the TILA interpretive rule recommended that the CFPB clarify that nonbank BNPL providers are held to the same standards as banks with regard to consumer protections generally.

With regards to pass-through payments, bank data providers, a large nondepository data provider, and trades representing bank and nondepository data providers stated that data related

[49] *Truth in Lending (Regulation Z); Use of Digital User Accounts To Access Buy Now, Pay Later Loans*, 89 FR 47068 (May 31, 2024).

to those products would be duplicative, introduce errors, provide limited consumer benefit relative to the increased burden on digital wallet providers, and conflict with their belief that the account-holding bank should control access to that data. One data provider trade association asserted that data providers should only be permitted to share data that is unique to them. The commenter stated that banks cannot conduct due diligence on the authorized third party that is requesting data access through the digital wallet provider, and this could lead to consumer confusion and other risks. The commenter asserted that these digital wallets do not possess data pertaining to a consumer financial product or service that the consumer obtained from the data provider. Some bank data provider commenters cited security and liability concerns about allowing pass-through payment providers to share data with third parties, rather than requiring the third parties to go to the underlying bank.

A few commenters stated that the proposal was unclear as to whether any entity that controls or possesses covered data would have obligations under the rule, even if a consumer did not obtain a covered consumer financial product or service from the data provider and even if the data do not concern a covered consumer financial product or service. A few trade associations and other commenters asserted that the CFPB needed to clarify whether point of sale terminal providers and other payment service providers are covered under § 1033.111(c). One bank trade association asked the CFPB to clarify that the obligation to make available covered data would not apply to consumers who are domiciled outside of the U.S., stating that without this clarification foreign requirements for data protection and privacy will be triggered, impacting data handling and protection that vary widely across countries.

The CFPB received many comments from individual consumers, consumer groups, other nonprofit organizations, third parties, and Members of Congress in support of covering EBT

providers in this stage of the rulemaking. Their reasons were similar to those raised during the SBREFA process, including how consumers would benefit from increased access to their EBT data and how such access could help identify fraud. Some of these commenters also asserted that excluding EBT providers from this rulemaking could worsen existing issues related to data access and service. A few commenters supported a subsequent rulemaking to cover EBT providers if they are not covered under this rule.

Some commenters, including industry trade associations and a Member of Congress, cautioned against including EBT providers in this or any future rulemaking. Although these commenters raised concerns the CFPB considered in the proposed rule, like the potential for fraud to increase and the lack of EFTA protections, some commenters also asserted that the CFPB is not the right agency to address EBT data access. These commenters asserted that Congress specifically excluded EBT from being regulated as demand deposit accounts and instead largely granted authority to regulate EBT to USDA. A payments trade association commenter cautioned that agencies that administer EBT will not have contractual relationships with entities involved with third party access and therefore these entities will not need to comply with certain restrictions put in place by the governing agencies.

Final rule

For the reasons discussed herein, the CFPB is finalizing § 1033.111(a) through (c) as proposed, with some clarifying changes to the definition of covered consumer financial product or service in § 1033.111(b)(3). This facilitation of payments prong in § 1033.111(b)(3) is finalized to include facilitation of payments from a Regulation E account or Regulation Z credit card, excluding products or services that merely facilitate first party payments. For purposes of

part 1033, a first party payment is a transfer initiated by the payee or an agent acting on behalf of the underlying payee. First party payments include payments initiated by loan servicers.

As in the proposal, § 1033.111(c) defines data provider to mean a covered person, as defined in 12 U.S.C. 5481(6), that is: (1) A financial institution, as defined in Regulation E, 12 CFR 1005.2(i); (2) A card issuer, as defined in Regulation Z, 12 CFR 1026.2(a)(7); or (3) Any other person that controls or possesses information concerning a covered consumer financial product or service that the consumer obtained from that person. Example 1 to paragraph (c) states that a digital wallet provider is a data provider.

Payment data from these products and services support common beneficial consumer use cases today, including transaction-based underwriting, payments, deposit account switching, and comparison shopping for bank and credit card accounts. Data from checking accounts, savings accounts, and other Regulation E accounts allow a consumer or third party to view a consumer's income, expenses, fees, and spending. Digital wallet providers hold similar valuable data that can provide a complete understanding of a consumer's finances. Today, a digital wallet can initiate payments from multiple credit cards, prepaid accounts, and checking accounts. A digital wallet can facilitate payments from accounts that the digital wallet provider offers through depository institution partners, or from linked accounts issued by other institutions (sometimes referred to as pass-through payments). Regulation Z credit cards are increasingly used as payment devices for everyday expenses, and credit card transaction data have in some cases become interchangeable with Regulation E account transaction data. Given the foreign applicability provisions of Regulation E and Regulation Z, covered consumer financial products and services in this rule are limited to products and services obtained by consumers who reside in the U.S. See Regulation E comment 3(a)-3 and Regulation Z comment 1(c)-1 for a discussion of foreign applicability.

Covering Regulation E accounts, Regulation Z credit cards, and payment facilitation products and services leverage existing infrastructure for consumer-authorized data sharing, thus facilitating implementation. Data providers generally share these covered data on consumer interfaces today, and some share covered data with third parties. Given how consumers' payment data are commonly shared and can be used to access consumer funds or track household spending, it is appropriate to prioritize these data for greater protection under this rule. As discussed in part IV.C and D, the CFPB is also finalizing a number of measures to foster a safe and secure data access framework.

In addition, consumers benefit from being able to permission access to digital wallet pass-through data and the marginal burden on digital wallet providers is generally limited. Digital wallet providers and entities that refer to themselves as neobanks generally qualify as Regulation E financial institutions; some also may be Regulation Z card issuers. Digital wallet providers that facilitate pass-through payments typically also provide a funds-holding asset account or credit card, so would already be subject to the requirements of this rule, including the requirement to maintain interfaces under § 1033.301. The few digital wallet providers who do not yet offer these products in conjunction with their pass-through products tend to be very large, sophisticated technology companies that commonly access and use data as third parties. Although digital wallet providers today typically qualify as Regulation E financial institutions under § 1033.111(c)(1), including § 1033.111(c)(3) provides clarity that all digital wallet providers are data providers and ensures coverage as payment products evolve. This provision makes clear that the rule covers consumer-facing entities involved in facilitating Regulation E account and Regulation Z credit card transactions, except, as discussed below, products or services that merely facilitate first party payments. Given that digital wallet providers—including

pass-through providers—typically are Regulation E financial institutions, the marginal compliance burden of including the payment facilitation prong is limited.

Moreover, the potential consumer benefit is clear. Digital wallets are ubiquitous today, with both remote and point of sale acceptance. Some companies that originated as non-financial providers, such as search engines, social media companies, and retail merchants, are steadily offering asset accounts and credit cards themselves—sometimes leveraging data they have obtained from depository institutions for underwriting or other purposes. As consumers increasingly connect multiple financial products to these non-bank providers, and these providers increasingly offer asset accounts and credit cards in conjunction with other services, non-bank providers may control or possess different or more robust covered data than the underlying depository institution. Consumers may also find it more convenient to permission access through the digital wallet provider or other payment facilitation provider, and may expect to be able to do so. Accordingly, requiring digital wallet data providers to make available data for both pass through and non-pass through accounts may best align the rule with consumer expectations, ease sharing for consumers who connect multiple payment methods to their digital wallets or otherwise frequently use their digital wallets, and provide consumers with access to more robust payment transaction data. The CFPB agrees with commenters that pass-through data providers should not be required to make available information to initiate payment to or from a Regulation E account under § 1033.211(c); changes to the covered data provision are discussed below in connection with subpart B.

The CFPB is clarifying the definition of covered consumer financial product or service in § 1033.111(b)(3) to exclude situations where an entity is solely facilitating first party payments, such as a merchant or mortgage loan servicer initiating a payment from the consumer's account

to itself. First party payments are distinct from payment facilitation products. Accordingly, the CFPB is finalizing § 1033.111(b)(3) with language to explicitly exclude products or services that merely facilitate first party payments. For purposes of this definition, a first party payment is a transfer initiated by the payee or an agent on behalf of the underlying payee. First party payments include payments initiated by a loan servicer.

Situations where an entity is merely initiating a payment to itself for a product or service it provided to the consumer would not be enough to qualify as a covered consumer financial product or service. For example, a mortgage servicer that merely initiates a payment to fulfill the consumer's mortgage obligation would not qualify as facilitation of payments under § 1033.111(b)(3), as the mortgage servicer is initiating a payment to itself or is otherwise acting an agent to the underlying mortgage holder. Similarly, an online merchant initiating a payment to itself for goods it sold directly to the consumer, or a utility company initiating payment to satisfy a consumer's electric bill, would not qualify as facilitation of payments under § 1033.111(b)(3). However, some first party payments continue to fall within the definition of covered consumer financial product or service, such as situations where the data provider is initiating a transfer to itself in conjunction with a product that facilitates payments to other payees, or the data provider is otherwise providing a Regulation E or Regulation Z account. For example, § 1033.111(b) includes a digital wallet provider initiating a transfer from an external bank account to the consumer's digital wallet held by that same provider, a digital wallet provider initiating a pass through transfer from the consumer's Regulation E or Regulation Z account to another payee that participates in the debit or credit card network, and a credit card provider initiating a credit card payment from the consumer's external bank account to itself.

As stated in § 1033.201(a)(1), a data provider's obligation to make available data is limited to 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, in an electronic form usable by consumers and authorized third parties. For clarity, the CFPB is adding language to § 1033.111(a) to reiterate that a data provider's obligations are limited to covered data concerning a covered consumer financial product or service that the consumer obtained from the data provider.

With regard to excluding products that are not subject to the CFPB's authority, any such exclusions would be superfluous, potentially confusing, and create risk that they would be misused to undermine coverage of payment facilitation products that do fall within the CFPB's authority. The § 1033.111(b) definition of covered consumer financial product or service is expressly limited to a consumer financial product or service as defined in 12 U.S.C. 5481(5). The CFPB has decided not to add exclusions, such as an exclusion for online marketplaces that are not otherwise subject to the CFPB's authority, because that may create detrimental loopholes for products that also provide a payment facilitation or other Regulation E access device function. For example, an online marketplace may involve payments to the data provider for products or services sold by that same data provider, but also facilitate payments to other merchants.

The CFPB intends to implement CFPA section 1033 with respect to other covered persons and consumer financial products or services through future rulemaking. The CFPB declines to expand the scope of covered data and consumer financial products and services in this final rule. Prioritizing Regulation E accounts, Regulation Z credit cards, and payment facilitation products and services advances competition goals across a broader range of markets while addressing pressing consumer use cases and risks. The CFPB also has considered that the

marginal risks to consumers of including these covered consumer financial products and services is limited by Regulation E and Regulation Z error protections applying to all the products covered by this final rule; in addition, most (if not all) such covered data are shared with third parties to some extent today. The CFPB has considered that EBT cards are exempt from EFTA coverage by statute, but that pursuant to the Consolidated Appropriations Act of 2023, the USDA has been directed to engage in a rulemaking and issue guidance on EBT card security practices. The Spring 2024 Unified Agenda shows that this USDA rulemaking is in the proposed rulemaking stage, indicating that completion of a final rule remains some period away.

In order to determine coverage, entities need to determine whether they control or possess covered data concerning a covered consumer financial product or service that the consumer obtained from that entity, and whether they otherwise meet the definition of data provider in § 1033.111(c). This coverage determination is the same for all entities, including those that in providing BNPL products may qualify as card issuers under Regulation Z. BNPL providers had sufficient notice of their potential inclusion in the rule because they received notice that the CFPB proposed to cover Regulation Z card issuers and credit cards under CFPA section 1033.

4. Coverage threshold for depository institution data providers (§ 1033.111(d))

Proposal

In § 1033.111(d), the CFPB proposed to exclude from the requirements of this rule data providers that are depository institutions without a consumer interface. The CFPB noted that such institutions tend to be very small, may not have resources to support or maintain online or mobile banking systems, and may use a relationship banking model that provides a more personalized relationship with their customers. The CFPB also proposed to limit the exclusion to depository institutions, preliminarily determining that the complicating factors that exist for

depository institutions are less likely to exist for nondepository institutions. The proposed rule also noted that nondepository institution data providers within the scope of the proposed rule tend to use business models built on the ability to innovate using technology and to move quickly to implement technological solutions. The CFPB sought comment on various issues, including whether different or additional criteria, such as an institution's asset size or activity level, should be taken into consideration when determining what depository institutions would be covered by the rule.

Comments received

Though a few commenters stated that all institutions should be required to comply with the rule, the vast majority of those who commented on this provision stated that some institutions should not. Many credit union, bank, and credit union and bank trade associations commenters stated that the proposed exemption was too limited. Many of these commenters also stated that coverage should be based on asset size, instead of the presence of a consumer interface, and suggested thresholds ranging from $850 million to $10 billion in total assets. Others stated that number of deposit accounts or customers should be relevant to coverage, or that depository institutions under a certain size should be able to "opt out" of the rule's requirements. A few credit union trade association commenters and one credit union commenter stated that there should be tiered exemptions where different tiers of depository institutions would not need to comply with various requirements of the rule: data providers with no consumer interface should be completely excluded, depository institutions that meet the SBA definition of a small business should only be required to provide a consumer interface, and minimum technical specifications should not apply to developer interfaces of depository institutions holding less than $50 billion in assets.

Several nondepository entity trade association commenters and one technology service provider commenter stated that nondepository institutions that do not have digital banking should be exempt from the rule. One nondepository institution trade association commenter stated that there are many nondepository institutions that do not have a consumer interface, including debt collectors.

While one bank commenter stated that depository institutions that elect to eliminate their consumer interfaces after the rule's effective date should not remain subject to the rule, a nondepository entity trade association commenter stated that they should. One nondepository entity trade association commenter stated that depository institutions should be given a grace period to comply with the rule's requirements when establishing a consumer interface while another stated that they should not. Finally, SBA Advocacy stated that the CFPB should consider third party exemptions that will not compromise data security and privacy.

Final rule

For the reasons discussed herein, the CFPB is finalizing § 1033.111(d) with modifications. Unlike the proposed rule, final § 1033.111(d) bases coverage on a depository institution data provider's total assets, not on the presence of a consumer interface. As in the proposed rule, all nondepository institution data providers are covered by the rule.

Final § 1033.111(d) states that the requirements of subparts B and C do not apply to data providers defined under § 1033.111(c)(1) through (3) that are depository institutions that hold total assets equal to or less than the SBA size standard for the data provider's appropriate NAICS code for commercial banking, credit unions, savings institutions and other depository credit intermediation, or credit card issuing, as codified in 13 CFR 121.201. The current size standard for all the relevant NAICS codes is $850 million. Section 1033.111(d) also states that, if at any

point, a depository institution that held total assets greater than that SBA size standard as of the final rule's effective date, subsequently holds total assets below that amount, the requirements of subparts B and C continue to apply. Section 1033.111(d)(1) provides information on how to determine the SBA standard based on specific NAICS codes. Section 1033.111(d)(2) explains that total assets held by a depository institution are determined by averaging the assets reported on its four preceding quarterly call report data submissions to the FFIEC or NCUA, as applicable, or its submissions to the appropriate oversight body to the extent it does not submit such reports to the FFIEC or NCUA. Relatedly, and as more fully discussed in the discussion of compliance dates, § 1033.121(c) addresses how to determine compliance dates for depository institutions that hold total assets at or below the SBA size standard but that subsequently cross that threshold.

Unlike the proposed rule, the final rule bases coverage on the total assets held by a depository institution data provider and provides those entities a reasonable amount of time to comply with the part's requirements upon reaching the coverage floor. Asset size is a more accurate proxy than the mere existence of a consumer interface to help approximate a depository institution's resources and ability to comply with the rule's requirements. An institution that may offer a basic consumer interface may nevertheless not possess the resources or technological sophistication to upgrade that interface and create a compliant developer interface. A depository institution's total asset size, however, provides information about an institution's size, sophistication, and relative resources to comply with the rule because an institution's size measured by assets will generally correlate with its resources. In addition, the CFPB does not

have information to indicate that any depository institution data provider over the current $850 million size standard lacks a consumer interface.[50]

Under the final rule, to streamline compliance, the specified depository institution data providers are not subject to any requirement to make data available through an interface. However, most depository institution data providers with total assets at or below the current $850 million size standards already have some form of consumer interface, and the CFPB expects that such institutions will continue to provide their customers with that service. The CFPB also understands that many depository institution data providers with total assets at or below the current $850 million size standards make at least some covered data available to consumer-authorized third parties, and expects that such institutions will continue doing so, including by offering developer interfaces when the benefits of doing so are commensurate with the institution's resources.

As with the proposed rule, the final rule covers all nondepository institution data providers. Though a few commenters stated that nondepository institution data providers without consumer interfaces should not be covered by the rule's requirements, they did not offer grounds to rebut the proposed rule's determination that nondepository institution data providers lack the same complicating factors that exist for their depository institution counterparts. Nondepository institution data providers within the scope of the final rule tend to use business models built on the ability to innovate with respect to technology and move quickly to implement technological changes and solutions.

[50] If there were hypothetically such depository institutions, their number would be very small and creating an exemption solely for such institutions would add complexity to the regulatory regime and not be proportionate.

As explained, the final rule does not cover depository institution data providers that hold total assets below the SBA size standard for the specific NAICS code that encompasses each depository institution data provider subject to this rule. The size standard for each of the named NAICS codes, currently $850 million, is re-evaluated by the SBA at least once every five years. In theory, the size standards of the named NAICS codes could diverge during that re-evaluation. The CFPB has determined that, given the historical standards, the likelihood of that occurring is minimal.

The CFPB believes the SBA size standard is an appropriate threshold to determine depository institution data provider coverage at this time. Several credit union trade associations and a trade association of community banks stated that an $850 million threshold would address concerns about the costs of providing data access to third parties under the terms of the rule. In particular, a credit union trade association believed such a threshold would be appropriate to address concerns about the ability of smaller credit unions to remain competitive, noting that those below the threshold might discontinue services if they had to comply with the rule. As discussed further in part VI.E.1, many community banks, credit unions, and trade associations commented that they expect the costs for small depository institutions of providing required data access to be much higher than those estimated by the CFPB in the proposal. Though they did not provide additional data or information that would allow the CFPB to precisely update the cost estimates, the CFPB acknowledges that small depository institutions might face additional challenges in implementing the rule at this time. The CFPB believes that the SBA size standard is an appropriate metric to ensure the rule does not unduly burden entities that are not dominant in their field and may have difficulty competing under the rule without sacrificing products or services.

At least one bank trade association commenter recommended generally that the coverage threshold be $10 billion in total assets, although the commenter stated that if the threshold is not set at $10 billion, then an asset threshold of $850 million would be appropriate.[51] This commenter did not provide reasoning for this position, and based on other comments received, the CFPB believes depository institutions with assets above the SBA size standard in the final rule will not face the same types of constraints as those below. For example, a credit union trade association recommended that credit unions with assets between $850 million and $50 billion should be subject to the data provider requirements of the rule, with the exception of minimum technical performance requirements. As discussed in part IV.C.3, the CFPB has made the minimum response rate requirement in § 1033.311(c) more flexible relative to the proposal and has lengthened the compliance timelines for all data providers. Further, not covering depository institutions with total assets of $10 billion and under would not cover a large share of total accounts, at approximately 31 percent of covered accounts. In contrast, setting the threshold at depository institutions with more than $850 million in total assets excludes approximately 10 percent of covered accounts.

For now, in light of the reasons herein, the CFPB is not extending coverage to depository institutions with assets of $850 million or below. However, the CFPB anticipates that, as the process of building out systems capable of complying with the rule's requirements plays out and data providers, core providers, and other vendors work to streamline the resources and processes necessary to comply, the costs of compliance will go down, potentially making coverage for smaller depository institutions more appropriate. Relative to the alternative of a higher coverage

[51] The CFPB also received one comment from a software developer stating that, until an accreditation process has been developed, financial institutions with less than $10 billion in assets should not be required to comply with the rule.

threshold such as $10 billion in assets, covering a larger share of depository institution data providers with this rule—and, in particular, covering depository institution data providers that use the same vendors and core providers as smaller depository institutions—increases the likelihood that resources to facilitate third party access will be available for smaller depository institution data providers that seek to integrate them in the future. The CFPB will continue to monitor market conditions and engage with relevant vendors and other service providers to determine if changes to the rule's coverage are warranted.

Section 1033.111(d)(2) states that a depository institution data provider's total assets are calculated by averaging its assets reported on its four preceding quarterly call report submissions to the FFIEC or NCUA, as applicable. Averaging total assets over a year provides a more accurate financial picture than using the total assets at one point in time. Additionally, the SBA calculates whether a specific institution meets its size standards by averaging the assets reported on its four quarterly financial statements for the preceding year. *See* 13 CFR 121.201 n.8.

Section 1033.111(d)(3) outlines the process by which a depository institution data provider determines total assets when there is a merger or acquisition where the surviving depository institution does not have four quarterly call report submissions. The surviving depository institution shall use the combined assets reported on the quarterly call report submissions by all predecessor depository institutions for quarterly assets prior to the merger. For quarterly assets after the merger or acquisition, quarterly assets shall be determined by using the assets reported on the quarterly call report submissions by the surviving depository institution. Total assets shall be determined by using the average of the quarterly assets for the four preceding quarters, whether the quarterly assets are the combined assets of the predecessor depository institutions or from the surviving depository institution. The rule does not include

explicit instructions on how newly formed depository institution data providers with no predecessor depository institutions determine total assets. The regulatory text is clear that four quarterly call report submissions are necessary to determine total assets and thus, a newly formed depository institution data provider with no predecessor depository institutions will determine total assets once it has four of its quarterly call report submissions available to make that determination.

As of the rule's effective date, depository institution data providers must determine their total assets by averaging their assets on the four preceding call report data submissions. If that total falls under the coverage threshold, the institution is not then subject to the rule's requirements, but it must continue to calculate total assets going forward based on the formula laid out in § 1033.111(d)(2) to determine if its assets have increased enough such that it becomes covered by the rule.[52]

The final rule does not allow depository institution data providers to fall out of coverage because their asset holdings dip from above to below the threshold. Once a depository institution data provider has become capable of building and maintaining data access in accordance with the rule's requirements, it will need to meet the data access requirements of the rule; ongoing costs of compliance will be minimal, even if their total assets held have diminished.

5. Compliance dates (§ 1033.121)

Proposal

The CFPB proposed in § 1033.121 to stagger data provider compliance dates into four tiers, so as to ensure timely compliance based on asset size or revenue, depending on the type of

[52] Section 1033.121(c) describes compliance dates for depository institution data providers that hold total assets less than the SBA size standard as of the effective date but subsequently cross that threshold.

data provider. A number of factors might affect how quickly a data provider could comply with the rule, including, for example, a data provider's size, relative technological sophistication, use of third party service providers to build and maintain software and hardware systems, and, in the case of many data providers, the existence of multiple legacy hardware and software systems that increase cost or otherwise impact their ability to layer on new technology. Nondepository institution data providers do not face these same obstacles. They do not have as many vendors and information technology systems that would need to be connected, and implementation could generally occur in-house. Thus, they could move faster to implement the rule's requirements. In preamble, the CFPB noted that data providers might need to transition third parties to developer interfaces in a staggered order; proposed § 1033.321 provided flexibility in that respect.

Subject to the limitations of proposed §§ 1033.321 and 1033.111(d), proposed § 1033.121 would have required data providers to make data access available by four compliance dates, all tied to publication of the final rule in the *Federal Register*: (1) depository institutions with $500 billion in total assets and nondepository institutions that generate $10 billion in revenue in the preceding calendar year or that are projected to generate $10 billion in revenue in the current calendar year would have been required to comply approximately six months after *Federal Register* publication; (2) depository institutions with between $50 billion and $500 billion in total assets and nondepository institutions that generate less than $10 billion in the preceding calendar year and are projected to generate less than $10 billion in the current calendar year would have been required to comply approximately one year after *Federal Register* publication; (3) depository institutions with between $850 million and $50 billion in total assets would have been required to comply approximately 2.5 years after *Federal Register* publication;

and (4) depository institutions with under $850 million in total assets would have been required to comply approximately four years after *Federal Register* publication.

The CFPB sought comment on a number of issues, including whether different or additional criteria should be taken into consideration when determining compliance dates, on the structure of each tier, and whether nondepository institutions should be included in all tiers. The CFPB also sought comment on whether the final rule should include language clarifying the time allowed to fully transition third parties to data access, so as to ensure that data providers do not impede timely third party access to an interface while also accounting for reasonable risk management.

Comments received

Most commenters that addressed this section stated that a tiered implementation schedule was appropriate, while a few nondepository entity trade association, consumer advocate, and bank trade association and bank commenters stated that such implementation would incentivize data aggregators and third parties to prioritize and work with larger entities and would temporarily create gaps in consumer data access across the market. One consumer advocate commenter also stated that tiered compliance may inadvertently disadvantage smaller institutions because the current speed of digital transformation can benefit larger, more resourced providers who will have a head start on developing norms for interfaces while less resourced providers will have less of a say in how those interfaces are developed. A nondepository entity trade association and a research institute commenter suggested that the CFPB should allow transition time once an API is available to move access gradually to the API and provide for a transition period rather than final compliance dates. Commenters did not specify how the final rule should structure a transition period without final compliance dates. A data aggregator and a third party

nondepository entity commenter also suggested that the final rule impose different compliance dates on different requirements in the final rule. One data aggregator commenter suggested specific API endpoints by which to set different deadlines for specific separate requirements.

Most commenters who addressed this section recommended that compliance dates account for the timeline for development of consensus standards (with some specific suggestions regarding standard file format and developer interface standardized format) and occur after the CFPB's recognition of a standard setting body, occur after the issuance of a qualified industry standard, or some combination of the above. See the discussion of § 1033.311(b) in part IV.C.3 below regarding the timing of the issuance of consensus standards by recognized standard setters.

Though a consumer advocate and a couple third party nondepository commenters saw the proposed compliance dates as appropriate, the majority of commenters, including banks, credit unions, credit union and bank trade associations, and nondepository entity trade associations, on this section described them as too short. Commenters explained that data providers would need to work with third parties, taking care not to put existing consumer account connections at risk when migrating and onboarding third parties to compliant data access, and would also need to ensure compliance with other rules, including any FCRA rules issued by the CFPB. Bank, credit union, and bank and credit union trade association commenters also noted many other actions data providers would have to engage in to comply, including updating public-facing websites to meet disclosure requirements, generating and publishing performance metrics, ensuring data are provided in a standardized format, ensuring support for required data elements that are not currently shared, build new functionality pertaining to machine-readable files accessible for consumers, and managing new access duration requirements, among other actions. Credit union

trade association commenters described the potential for a bottleneck in the proposed third tier because it would cover over 1,000 banks and credit unions, and requested an additional tier that would allow five years for implementation. One bank commenter stated that banks with less than $10 billion in total assets exclusively rely on third parties to provide digital banking, including bill payment portals, and core processing systems. One law firm commenter stated that nondepository institution data providers would have the most burden in complying because they are less likely to already have interfaces and policies in place to timely receive and respond to requests for data. Different commenters offered various time periods for how long compliance should be. Suggestions ranged from allowing an additional six to 18 months for all tiers, 24 months for the largest data providers, four to six years for small providers, and at least 10 years for all data providers.

Some bank, bank trade association, third party nondepository entity, and nondepository entity trade association commenters requested compliance dates for third parties and aggregators. One stated that the CFPB should ensure that the compliance date for the largest data providers is feasible not only for the relevant data providers but also for data recipients. Another stated that there should be a 12-month compliance period for aggregators and merchants that use aggregators, and a six-month grace period thereafter for aggregators to cure any technical violations that do not result in direct instances of consumer harm.

Finally, one bank trade association commenter asked for clarification as to how ownership structure influences which tier an entity falls into as some entities are comprised of multiple types of companies.

Final rule

For the reasons discussed herein, the CFPB is finalizing § 1033.121 with revisions to increase the number of compliance date tiers, redefine the types of depository institutions included in each tier, change the metrics used to define the types of data providers included in each tier, extend compliance deadlines for all tiers, and provide clarification for how depository institution data providers determine compliance deadlines when their total assets do not meet the threshold for coverage as of the effective date but subsequently cross that threshold. Specifically, § 1033.121(b) provides that, in the first tier, depository institution data providers that hold at least $250 billion in total assets and nondepository institution data providers that generated at least $10 billion in total receipts in either calendar year 2023 or calendar year 2024 must comply by April 1, 2026. In the second tier, depository institution data providers that hold at least $10 billion in total assets but less than $250 billion in total assets and nondepository institution data providers that generated less than $10 billion in total receipts in both calendar year 2023 and calendar year 2024 must comply by April 1, 2027. In the third tier, depository institution data providers that hold at least $3 billion in total assets but less than $10 billion in total assets must comply by April 1, 2028. In the fourth tier, depository institution data providers that hold at least $1.5 billion in total assets but less than $3 billion in total assets must comply by April 1, 2029. In the final tier, depository institution data providers that hold less than $1.5 billion in total assets but more than $850 million in total assets must comply by April 1, 2030.

Data providers must have established functioning developer and consumer interfaces required under § 1033.301(a) that are technically capable of complying with the requirements in subparts B and C of part 1033 by their compliance deadline. For example, developer interfaces must be able to make available all covered data (as defined in § 1033.211) in a standardized

format (§ 1033.311(b)) and be capable of performing in a commercially reasonable manner (§ 1033.311(c)). Some data providers will be able to receive requests from authorized third parties for covered data through their developer interface by then. However, the CFPB recognizes that other data providers may need to transition existing third party access arrangements or otherwise onboard new third parties after their compliance deadline as necessary to avoid violating other legal obligations and to manage the technical integration process.

The CFPB recognizes that data providers may need time to onboard third parties in a staggered manner in accordance with sound risk management. It is permissible under the final rule to manage the onboarding process a staged manner, to the extent permitted under § 1033.321. As discussed further in part IV.C.4 below, a data provider could rely on § 1033.321 to deny a third party access to the developer interface temporarily, consistent with policies and procedures reasonably designed to comply with safety and soundness standards of a prudential regulator (among other legal obligations), and if the denial complies with § 1033.321(b). Once a third party has access to the developer interface, a data provider must respond to requests for covered data in accordance with the rule.

It will raise significant concerns if a data provider seeks to rely on § 1033.321 to justify noncompliance with the technical requirements of subparts B and C of the final rule, such as those impacting functionality, commercially reasonable performance, or security of the developer interface. Such requirements are independent of whether a data provider can deny a third party access under § 1033.321. For example, it likely would be impermissible for a data provider to deny a third party access under § 1033.321 temporarily, in connection with onboarding, solely because the data provider's developer interface could not scale to achieve the

99.5 percent response rate required under § 1033.311(c)(1) for periods with a high volume of requests.

To be clear, § 1033.321 does not allow data providers to delay access during the onboarding process unreasonably. For example, a data provider could not manage the onboarding process in an inconsistent or discriminatory manner. Establishing policies and procedures to manage the onboarding process as expeditiously as possible in a way that properly accounts for relevant risk management considerations will help ensure data providers do not unlawfully avoid their obligations to implement CFPA section 1033. In managing the onboarding process, data providers are also subject to the rule's anti-evasion provision in § 1033.201(a)(2) and other applicable consumer financial laws, including the prohibition on unfair, deceptive, or abusive acts or practices.

Section 1033.121(a) provides that a data provider's compliance date is based upon the calculation of total assets or total receipts, as appropriate. Section 1033.121(a)(1) also provides that, for depository institution data providers, total assets are determined by averaging the assets reported on its 2023 third quarter, 2023 fourth quarter, 2024 first quarter, and 2024 second quarter call report data submissions to the FFIEC or NCUA, as applicable, or its submissions to the appropriate oversight body to the extent it does not submit such reports to the FFIEC or NCUA. With respect a commenter's request to clarify how ownership structure influences which tier a depository institution falls into for compliance purposes, the regulatory text makes clear that a depository institution data provider looks to the total assets it reports on its call report data submissions. Section 1033.121(a)(2) provides that, for nondepository institution data providers, total receipts are calculated based on the SBA definition of receipts, as codified in 13 CFR 121.104(a). Section 1033.121(c) states compliance timelines for depository institution data

providers that do not meet the coverage threshold as of the rule's effective date, but that subsequently cross that threshold. It provides that a depository institution data provider has a reasonable amount of time to comply with the rule after exceeding the size standard, and that the reasonable amount of time shall not exceed five years. This period is counted from the submission of a data provider's fourth call report described in the asset size calculation in § 1033.111(d)(2), the analysis of which, under such calculation, results in an asset size that crosses the size threshold.

The compliance periods for each tier in the final rule will ensure that data providers of different sizes and resources will have the appropriate amount of time to comply, in part, because the largest, most resourced data providers will be complying first and smaller depository institution data providers who are most likely to be relying on core providers and other third parties will be split into additional, smaller, more manageable tiers. The largest data providers, many of which already have the required interfaces in development, have until April 1, 2026, to comply, which will provide them with sufficient time to meet the rule's requirements. Comments received from the largest depository institution data providers, as well as data provider trade associations and a few smaller banks and credit unions, requested 24 months for the largest depository institution data providers to comply, but also noted that many of the largest depository institution data providers already have interfaces that could be adapted to comply with the final rule's requirements when issued and did not specify why 24 months would be necessary to build the developer interface required by the rule. In addition, some commenters requesting 24 months identified aspects of implementation related to onboarding third parties onto a developer interface and processing requests. As discussed above, data providers must

have established functioning interfaces by their compliance dates and are permitted to manage granting third parties access to the developer interface, consistent with § 1033.321.

The second tier of data providers will have more than two years to comply, which will allow them to learn from the experience coming into compliance of the first tier of data providers; the same is true for the third tier of data providers with more than three years for compliance. The fourth and fifth tiers, which constitute the smallest depository institution data providers by asset size and the entities most likely to depend on core processors or other third parties to assist with compliance, will be able to learn from the experiences of the data providers that had to comply earlier and should have a smoother transition than they might otherwise. These periods balance the need for effective compliance with the provision of sufficient time to ensure a smooth transition and minimize time between tier compliance to ensure that any temporary data access gaps will be short lived. The CFPB has revised the compliance date tiers in response to comments, to reduce the total number of depository institutions in each tier. This should reduce the burden on core processors and other third parties, easing overall compliance efforts.

Consistent with the proposed rule, nondepository institution data providers must comply with the final rule's requirements as part of the first or second tiers. But these tiers now have more time to achieve compliance. Further, though one law firm commenter stated that nondepository institution data providers are most likely not to already have interfaces and policies in place to timely receive and respond to requests for data, this assertion does not negate the CFPB's finding, through the SBREFA process and ongoing market monitoring, that such data providers do not have as many vendors and information technology systems that will need to be connected and that implementation by nondepository institution data providers can occur

in-house without the need to engage core processors or other third party vendors. These data providers also tend to have business models that are based on the ability to adopt to technological innovations relatively quickly. Thus, these data providers will be able to move more quickly to implement the rule's requirements.

The final rule clarifies that, for purposes of determining an institution's compliance date, a depository institution data provider must look at the average total assets over a defined year of call report data. Averaging total assets over the course of one year provides a more accurate picture of asset holdings than just using assets as of the end of a single calendar quarter. A nondepository institution data provider must look at its total receipts, as calculated based on the SBA definition of receipts in 13 CFR 121.104(a). The SBA definition of receipts is widely used in many regulations and provides a comprehensive, consistent definition for nondepository institution data providers to benchmark their revenue. These provisions will ensure that all institutions are using consistent metrics to determine compliance periods.

Section 1033.111(d) addresses asset limitations to coverage for depository institution data providers and specifies asset calculation methods. Section 1033.121(c) discusses compliance timing for depository institution data providers that are at or below the asset threshold at the effective date but later exceed the applicable threshold. This provision allows such institutions a reasonable time to comply after they exceed the applicable threshold, not to exceed five years. The smallest depository institution data providers subject to the rule's requirements as of the rule's effective date will have approximately five years to comply, making this a logical ceiling for compliance timing for depository institution data providers that subsequently become subject to the rule's requirements. However, as more time passes and more institutions implement the rule's requirements, compliance will become less onerous, less expensive and require less time.

Thus, what constitutes a reasonable amount of time for compliance may evolve downward with time.

The final rule does not set explicit compliance dates for third parties because they are unnecessary. The CFPB is providing additional time for the largest data providers to come into compliance with the rule, which will give third parties and aggregators additional time to prepare for implementation of the rule. In addition, transitioning the market from screen scraping will further incentivize third parties and aggregators to meet the requirements to request proper access under the terms of the rule. See part IV.4 above for a discussion of whether data providers complying with this rule are furnishers under the FCRA.

6. Definitions (§ 1033.131)

Card issuer, covered consumer financial product or service, covered data, data provider, financial institution, recognized standard setter, Regulation E account, and Regulation Z credit card

Consistent with the proposed rule, the coverage-related terms—card issuer, covered consumer financial product or service, covered data, data provider, financial institution, Regulation E account, and Regulation Z credit card—are listed under § 1033.131 with cross-references to the full definitions in §§ 1033.111 and 1033.211 (covered data).

The term recognized standard setter, which was finalized in the Industry Standard-Setting Final Rule, is also listed under § 1033.131 with a cross-reference to the full definition in § 1033.141. As finalized in that rule, the term refers to a standard-setting body with certain attributes listed in § 1033.141(a) (finalized as part of the Industry Standard-Setting Final Rule), including recognition by the CFPB pursuant to certain application procedures. The CFPB began accepting applications from standard-setting bodies seeking recognition in the summer of 2024.

Authorized third party

The CFPB proposed under section 1033(a) to require data providers to make available covered data to certain third parties "acting on behalf" of a consumer. The CFPB proposed in § 1033.131 to define the term authorized third party as a third party that has complied with the authorization procedures described in proposed § 1033.401. Proposed § 1033.401 specified what requirements a third party would have to satisfy to become an authorized third party, and thus be entitled to access covered data on behalf of a consumer.

Few commenters addressed the proposed definition of authorized third party. A third party commenter stated that data aggregators sometimes function as authorized third parties. The commenter recommended that the rule clarify how the definition applies to a data aggregator that follows the authorization procedures, stating that the definitions of authorized third party and data aggregator could be modified to note that an entity could be both. More generally, several commenters raised concerns about the scope of third parties that should be permitted under the rule to access covered data on behalf of consumers. These comments are addressed in part IV.D.1 below.

For the reasons discussed herein, the CFPB is adopting the definition of authorized third party as proposed to mean a third party that has complied with the authorization procedures in § 1033.401. As discussed in more detail in part IV.D, the authorization procedures are designed to ensure that third parties accessing covered data under section 1033(a) of the CFPA pursuant to the rule's framework are "acting on behalf" of a consumer, and therefore consistent with the definition of consumer in CFPA section 1002(4). This definition of an authorized third party provides a term to designate which third parties are entitled to access consumer information, on the consumer's behalf, pursuant to the rule's framework.

It is not necessary for the definition of authorized third party to specify that a data aggregator may also function as an authorized third party in other circumstances. A third party may play different roles in different circumstances. However, for a particular request for access to covered data, an entity would play only one role. The definition of authorized third party (like the definitions of data aggregator and data provider) is designed only to identify what role an entity plays for that particular request for access to covered data.

Consensus standard

The CFPB proposed in § 1033.131 to define the term qualified industry standard to mean a standard issued by a standard-setting body that is fair, open, and inclusive in accordance with § 1033.141(a), which includes CFPB recognition. In the Industry Standard-Setting final rule, the CFPB addressed comments regarding the proposed qualified industry standard definition, the attributes of a standard-setting body, and the process for CFPB recognition. The Industry Standard-Setting Final Rule revised the definition of qualified industry standard in proposed § 1033.131 and renamed it a "consensus standard."

While the Industry Standard-Setting Final Rule adopted this term, it did not address the role consensus standards would play in the final rule published in this *Federal Register* document. The CFPB generally proposed that conformance to a qualified industry standard would provide "indicia," or partial evidence, of data providers' and third parties' compliance with specified provisions. Generally, conformance to a qualified industry standard would not be required to comply nor would it constitute compliance with a specified provision.[53] No provision

[53] The one exception to that approach was with respect to the proposed requirement that a data provider's developer interface make covered data available in a "standardized format" in proposed § 1033.311(b). In that case, adherence to a qualified industry standard would have been deemed to satisfy the requirement. The final rule instead uses the indicia-of-compliance approach in that context, for the reasons explained in the discussion of final § 1033.311 below.

in the proposal would have required a data provider or third party to comply with a qualified industry standard.

Many commenters addressed the role consensus standards should play in the implementation of the final rule. Generally, commenters supported inclusion of standards set by voluntary standard-setting bodies, and focused on whether the standards should be indicia of compliance or something else, such as a safe harbor. Some commenters believed consensus standards should play no role in the final rulemaking and should rather be wholly determined by private standard-setting bodies.

One civil rights group commenter supported the proposal's approach to weighing standards as indicia of compliance. Further, data provider commenters preferred to consider compliance with consensus standards as an indicator of compliance rather than a requirement for compliance.

Some data provider and third party commenters recommended that consensus standards provide a legal safe harbor for compliance with various provisions of the final rule. These commenters suggested that a safe harbor would provide certainty and clarity to market participants and would encourage participants to invest in the setting of and compliance with appropriate standards. Further, commenters expressed concern that some participants may not expend the resources to conform to consensus standards if doing so could still result in noncompliance with regulatory requirements. Additionally, some bank commenters recommended that if the rule does not employ consensus standards as safe harbors, it should instead use a "commercially reasonable" standard. These commenters expressed concern that the "indicia of compliance" terminology could receive excessive weight by market participants, and effectively become the implicit compliance regime of the rule.

A variety of commenters opposed the framework for recognizing standard-setting bodies. Some commenters stated that CFPA section 1033 does not address the CFPB's authority to recognize standard-setting bodies as capable of issuing consensus standards for data providers and third parties, and that the proposed standards framework could conflict with prudential requirements imposed on data providers. One research institute commenter opposed the consensus standards framework on the grounds that the Federal government should not interfere with the internal governance of private standard-setting bodies.

Generally, the CFPB has determined that consensus standards can usefully serve as indicia of compliance for various provisions stated throughout the final rule. If the final rule provided safe harbors, as some commenters suggested, recognized standard setters could play a regulatory role, rather than a consensus standard-setting one. Such an approach would also ignore the fact that a standard may be insufficient in some respect (for example, for incompleteness given the rule requirement on point) or in particular, idiosyncratic circumstances. The indicia of compliance framework maintains part 1033 as the applicable legal standard while giving due weight to a fair, open, and inclusive consensus standard as evidence of compliance with the rule.[54] Consensus standards can assist entities in fulfilling their legal obligations but do not relieve an entity from its duty to confirm that it is complying with the rule.[55] By the same token, consensus standards are not mandates.

While some commenters advocated for a "commercially reasonable" test as a substitute for consensus standards, the CFPB believes that looking exclusively at commercial

[54] In this respect, the CFPB encourages recognized standard setters to ensure a consensus standard complies with the final rule and that they maintain procedures that allow regulated entities to straightforwardly evidence their conformance to a consensus standard at negligible cost.

[55] The CFPB may be able to provide additional guidance about particular consensus standards, especially if market participants seek that in particular cases. However, that is different from providing a safe harbor for all the consensus standards that may have some bearing on rule compliance, as requested by some commenters.

reasonableness would ignore the potential benefits of more specific consensus standards developed through a fair, open, and inclusive process involving all stakeholders. As discussed below, in the context of § 1033.311(c)(1), a developer interface must provide a response within a commercially reasonable amount of time and indicia of such a response includes conformance to an applicable consensus standard.

Regarding the comment opposing Federal government involvement in the governance of private standard-setting bodies, the CFPB notes that it has a legitimate interest in ensuring that standard-setting bodies follow an appropriate process when issuing standards as to which conformance carries some indicia of compliance with a CFPB rule. Moreover, no existing or future private entity is required to become a CFPB-recognized standard-setting body, and a range of external standards may continue to be of utility and value to regulated entities even if they are not consensus standards adopted by recognized standard setters. The CFPB is finalizing the provisions of the final rule that cite consensus standards using its rulemaking authority under CFPA section 1033(a) and (d) and section 1022(b)(1). These provisions carry out the objectives of section 1033 by encouraging the development of fair, open, and inclusive industry standards that will facilitate implementation of the final rule.

Regarding some commenters' concern that consensus standards could conflict with prudential requirements, CFPA section 1033(e) requires that the CFPB consult with the prudential regulators and the FTC so that certain objectives are met. In compliance with this provision, prior to issuing the Industry Standard-Setting Final Rule the CFPB consulted on several occasions with staff from the prudential regulators and the FTC to discuss various aspects of the rule, including criteria for and processes with respect to standard-setting bodies. Such discussions were, in part, to achieve effective alignment between the Industry Standard-Setting

Final Rule and prudential requirements. The CFPB has conducted further consultations after the release of the Industry Standard-Setting Final Rule and is not aware of conflicts with prudential requirements. In addition, because consensus standards serve as indicia, nothing in a consensus standard could legally override a Federal legal obligation, prudential or otherwise. A hypothesized conflict, accordingly, could not be meaningful.

Details about the role of consensus standards with regard to particular requirements of the final rule can be found in the discussion below.

Consumer

The CFPB proposed in § 1033.131 to define the term consumer for purposes of part 1033 to mean a natural person. The proposed definition specified that trusts established for tax or estate planning purposes would be considered natural persons. The preamble to the proposal explained that the proposed definition differs from the definition of consumer in CFPA section 1002(4), which defines a consumer as "an individual or an agent, trustee, or representative acting on behalf of an individual." The preamble explained the proposed definition was designed to distinguish the term consumer from third parties that are authorized to access covered data on behalf of a consumer pursuant to the proposed procedures in subpart D.

A bank and some trade associations for banks supported the proposed approach not to refer to "agents" in the definition of consumer, because they said including agents could cause significant confusion or complication as there are numerous parties which could act as the consumer's agent and would have access to covered data pursuant to the third party authorization procedures in subpart D. Some commenters, including third parties and data aggregators, noted what they described as potential confusion related to the proposed definition being different from

the statutory definition. Others, like data aggregators and third parties, stated that the final rule should align the definition of consumer to the statutory definition.

Commenters also asked for additional changes and clarifications related to the definition of consumer. For example, a data provider and trade associations for banks requested clarification around the proposed rule's inclusion of trusts established for tax or estate planning purposes as natural persons, and how a trust could authorize a third party to access the trust's data. Trade associations for third parties suggested the definition of consumer should be narrowed to include only consumers with at least one current account with the data provider. Additionally, a consumer advocate stated that the final rule should include in the definition of consumer small businesses seeking access to their financial data.

Finally, some banks, trade associations for data providers, third parties, and data aggregators focused on how smaller commercial third parties, or parties that traditionally would not require authorization through section 1033 to access consumer data, might be impacted by the rule (*e.g.*, how a small broker-dealer might be treated if they are not considered a consumer; and how custodians, guardians, and other authorized agents may authorize third parties).

For the reasons discussed herein, the CFPB is finalizing the definition of "consumer" in the rule as proposed with a modification to specify that the term includes guardians, trustees, custodians, or similar natural persons acting on behalf of a consumer pursuant to State law.

The term consumer is commonly used in various consumer finance-related contexts to refer to individuals, *i.e.*, natural persons. *See, e.g.*, Regulation E, 12 CFR 1005.2(e). The final rule accounts for the CFPA's definition, which also includes "an agent, trustee, or representative acting on behalf of an individual," by establishing third party authorization procedures described in subpart D to ensure all relevant parties may access covered data. Accordingly, the substance

of the rule aligns with the CFPA's definition of consumer, and nothing in the CFPA prevents the CFPB from using different vocabulary within such a rule.

Further, as described above, some commenters requested clarification regarding the inclusion of trusts as natural persons for purposes of the definition of consumer. Trusts are referred to as natural persons in other consumer finance-related contexts. *See, e.g.*, Regulation Z comment 3(a)-10 ("Credit extended for consumer purposes to certain trusts is considered to be credit extended to a natural person rather than credit extended to an organization."). In the context of CFPA section 1033, a data provider would control or possess the covered data concerning a consumer financial product or service that the trust obtained from the data provider. As such, trusts established for estate or tax planning purposes are appropriately considered consumers in the context of CFPA section 1033.

In the proposed rule, the CFPB requested comment on how individuals who are not account owners currently use existing legal mechanisms to directly access covered data. As described above, some commenters sought clarification on how parties that traditionally would not require authorization through CFPA section 1033 to access consumer data might be impacted by the rule. For example, some commenters cited guardians and custodians as examples of natural persons who might manage certain accounts and therefore attempt to authorize third parties to access covered data. After considering these comments, the CFPB is including in the definition of consumer a statement that consumers include guardians, trustees, custodians, or similar natural persons acting on behalf of a consumer pursuant to State law. In these circumstances, natural persons who manage consumer accounts through legal instrumentation are granted authority to manage those assets. Custodial accounts, for example, may be established by financial institutions under the Uniform Gifts to Minors Act (*see generally*

8A U.L.A. 405 (1983)) or the Uniform Transfers to Minors Act (*see generally* 8A U.L.A. 153 (Supp. 1987)), and are set up and managed by an adult for the benefit of a minor until the minor reaches the age of majority. Guardianships, trusts, and custodian accounts function similarly: existing legal processes, unrelated to CFPA section 1033's data access rights, establish rights for a natural person to manage the assets and income for another natural person. In these cases, it would be appropriate for the natural person duly authorized to manage another natural person's covered financial products or services to also authorize third parties to access the covered data related to those products or services pursuant to section 1033. Further, the State statutory and common law protections in place that cover these persons are sufficient such that these persons can be considered consumers when acting in those capacities for another person, and it is not necessary to apply the provisions of subpart D to them.

The CFPB is aware that some corporate terms and conditions contain provisions by which consumers purportedly appear to consent, upon acceptance, to the corporate entities' limited powers of attorney to act as agents for the consumers. These circumstances would not position such corporate entities as consumers under the revised definition in final § 1033.131 of the rule because they are factually and legally different from those circumstances addressed by the final rule's definition of consumer. The natural persons considered consumers under the final rule have broad authority established through State law mechanisms to stand directly in the shoes of the consumer with respect to the covered financial product or service associated with the consumer.

Finally, as described above, some commenters suggested the CFPB narrow the final rule to include only consumers with at least one current account with the data provider. The CFPB has determined that §§ 1033.201(a) and 1033.331 and the authorization procedures described in

§ 1033.401 sufficiently ensure that consumers who have covered data and accounts with the data provider can authorize third parties to access covered data, while the exceptions in CFPA section 1033(b) and § 1033.221 ensure that data providers are not required to provide information that they cannot provide in the ordinary course of business. A commenter also suggested the final rule include small businesses in the definition of consumer. However, CFPA section 1033 applies only to "consumer financial products and services" as defined in CFPA section 1002(5). Accordingly, expanding the final rule to include small business accounts would be inconsistent with the statutory text. However, the CFPB expects that small business account providers may find the framework of part 1033 to be a useful model for enabling small businesses to share data about their accounts, and therefore may choose to use their developer interfaces to facilitate that access.

Consumer interface

The CFPB proposed in § 1033.131 to define consumer interface as 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.

No commenters objected to the proposal's general approach of a framework under which authorized third parties would not be entitled under part 1033 to access individual consumers' covered data through providers' functionality designed for consumers. Depository institutions and depository institution trade associations stated, however, that the proposed definition was insufficiently clear because under the proposal a depository institution data provider would have been exempt from part 1033 if it did not have a consumer interface. They said that a data provider with relatively basic online banking functionality for its consumer account holders

would not be able to determine with sufficient certainty whether that functionality qualified as a "consumer interface" thereby subjecting the data provider to the requirements of part 1033.

Under the final rule, the application or non-application of part 1033 to a depository institution data provider does not depend in whole or in part on whether or not the data provider has functionality for providing covered data to individual consumers. Instead, as discussed elsewhere, it is determined by whether the data provider is above a certain asset size. As a result, a data provider above that asset size and thus subject to part 1033 does not need to determine whether the functionality through which it makes covered data available to individual consumers meets the definition, but instead must ensure that it offers functionality for making covered data available that meets the requirements of subparts B and C of part 1033.[56] Accordingly, the rule's label for that functionality—the "consumer interface" definition—does not need modification and the CFPB adopts the definition as proposed for the reasons discussed herein.

Data aggregator

The CFPB proposed in § 1033.131 to define the term data aggregator to mean an entity that is retained by and provides services to the authorized third party to enable access to covered data. The proposed rule noted that some third parties retain data aggregators for assistance in obtaining access to data from data providers. Certain provisions in proposed § 1033.431 specified what role data aggregators would play in the third party authorization procedures, what information about data aggregators would have to be included in the authorization disclosure, and what conditions data aggregators would have to certify that they agree to as part of the third party authorization procedures. The CFPB requested comment on whether data aggregator is an

[56] If a data provider has more than one mechanism through which it makes available covered data to consumers, each of the mechanisms does not individually need to satisfy the requirements of part 1033. Collectively, the mechanisms must do so.

appropriate term for describing third parties that may provide assistance in accessing covered data or whether there are other terms, such as "data intermediary," that would be more appropriate.

Some commenters stated that the proposed definition was too broad. A research institute commenter stated that the proposed definition would sweep in any service provider or subcontractor that contributes in any way to a third party being able to access consumer data from a data provider. The commenter recommended narrowing the definition to avoid imposing burdens on service providers that have no direct relationship to consumers or their data. A nondepository entity commenter stated that data aggregator is a generic term that could lead to confusion and recommended that the rule provide more granular definitions of the different types of services provided, with the term data aggregator applying only to entities that aggregate all types of financial data. A data aggregator commenter stated that the rule should use the term data access platform instead of data aggregator because the term data aggregator does not fully reflect the role that such entities play and that data access platform is a market standard term.

In contrast, a bank and a bank trade association commenter stated that the proposed definition of data aggregator was too narrow. The bank commenter requested that the definition of data aggregator be expanded to include data aggregators that assist non-authorized third parties in accessing consumer data.

Several commenters recommended that the CFPB clarify the proposed definition of data aggregator. A research institute commenter stated that the CFPB should clarify whether a data aggregator can be an authorized third party. Two credit union trade associations recommended that the rule clarify what "retained by" means in the context of a third party that uses a wholly owned subsidiary as a data aggregator, and also what "enable access to covered data" means for

a credentialing service that facilitates a data provider's risk management and data security review. Finally, they stated that the rule should clarify whether "enabling access" requires a data aggregator to be the party connected to a developer interface.

For the reasons discussed herein, the CFPB is finalizing the definition of data aggregator with a minor change from the proposal. The proposal defined data aggregator to mean an entity that is retained by and provides services to the authorized third party to enable access to covered data. The term "person" as used elsewhere in the rule and in the CFPA includes both natural persons and entities. In most situations, a data aggregator will be an entity rather than a natural person. However, to account for the situation in which a data aggregator is not an entity and for consistency with other definitions, such as third party, the CFPB is revising the definition to change "entity" to "person," so that data aggregator means a person that is retained by and provides services to the authorized third party to enable access to covered data. This definition of data aggregator strikes an appropriate balance. It is broad enough to include persons that provide various types of services to authorized third parties that enable access to covered data, ensuring that the consumer protections related to data aggregators will apply to persons involved in accessing and collecting covered data. It is not limited to persons that are connected to a developer interface, as it also covers persons collecting, processing, or combining covered data.

However, by limiting the scope of the definition to persons that provide services to the authorized third party to enable access to covered data, the definition avoids sweeping in persons that are providing services that are only incidentally connected to data access. Contrary to the concerns raised by one commenter, the definition does not cover a person that contributes in any way to accessing covered data; the person must provide services that enable access to covered data in order to meet the definition of a data aggregator. The CFPB has determined that it would

not be appropriate to adopt more granular definitions based on the specific services that entities provide. The purpose of the data aggregator definition is to identify persons that, regardless of the specific services they provide, are subject to various consumer protections in the rule because of their involvement with and proximity to covered data.

As noted above in connection with the discussion of the definition of authorized third party, the CFPB recognizes that persons may play different roles in different transactions and that an entity may be a data aggregator in some transactions and an authorized third party in others. The definitions of data aggregator and authorized third party are intended to identify what role an entity is playing with respect to a particular request for covered data and are not fixed terms. Regarding the comment about whether a wholly owned subsidiary of a third party could be a data aggregator, the CFPB notes that, assuming the subsidiary is a separate person from the third party, the subsidiary could be a data aggregator.

The CFPB declines to expand the scope of the data aggregator definition to include data aggregators that serve non-authorized third parties. The data aggregator definition, and the provisions related to data aggregators in § 1033.431, are designed to specify what obligations data aggregators must satisfy when they assist authorized third parties that access covered data on a consumer's behalf pursuant to the rule's framework. Expanding the definition of data aggregator to include persons that provide data aggregation services to non-authorized third parties would go beyond the scope of the consumer-authorized data access framework described in the rule.

The CFPB also declines to further expand upon what "enable access to covered data" means in specific contexts, as requested by some commenters. The definition is designed to capture a variety of different arrangements and accordingly is sufficiently clear. Finally, the

CFPB declines to adopt a term other than data aggregator. Only one commenter recommended using a different term, and data aggregator is a widely used and understood term.

Depository institution

The CFPB is adding a definition of depository institution to the final rule for clarity and to facilitate compliance with the rule. The definition of depository institution is any depository institution as defined in the Federal Deposit Insurance Act, 12 U.S.C. 1813(c)(1), or any credit union as defined in the NCUA's regulation at 12 CFR 700.2. This definition provides additional clarity that all depository institutions, not just bank entities, are included when the rule refers to depository institutions.

Developer interface

The CFPB proposed in § 1033.131 to define developer interface as 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.

Commenters generally did not express concern with the proposed definition. A few blockchain-related nondepository and individual consumer commenters, however, stated that the CFPB should require data providers to grant developer interface access to individual consumers upon the consumers' submission of sufficient information to the data providers (*i.e.*, sufficient to enable the providers to comply with their interface access and risk assessment obligations under part 1033 and other laws). These commenters said that such a requirement would help empower consumers to serve as their own personal financial data custodians if they so desire.

The final rule does not require data providers to grant developer interface access to individual consumers (though it also does not bar them from doing so). Such a requirement could burden data providers in ways the CFPB has not adequately evaluated by necessitating that they

consider a high number of requests for consumer access to their developer interfaces. In addition, consumers may obtain their financial data—including in machine-readable form—through consumer interfaces.

For the reasons discussed herein, the CFPB is finalizing the definition of developer interface as proposed. The definition does not require use of any particular technology. Instead, it facilitates the readability of part 1033 by establishing a brief label—"developer interface"—by which other provisions in part 1033 may refer to the functionality through which a data provider receives and responds to requests for covered data from authorized third parties in accordance with the requirements of the rule. The very limited comments on this definition indicate that relevant industry participants do not object to the utility of the term for these purposes.

Third party

The CFPB proposed in § 1033.131 to define the term third party as 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. The proposed rule used the term third party to refer to entities seeking access to covered data and to other parties, including data aggregators.

A trade association for nondepository entities stated that the definitions of third party and data provider (addressed in § 1033.111(c)) were unclear. The commenter stated that an entity could be construed as either, such as when a fintech partners with a bank.

For the reasons discussed herein, the CFPB is finalizing the definition of third party with a minor change from the proposal. The proposed definition referred to "any person or entity." The term "person" as used elsewhere in this rule and in the CFPA includes both natural persons and entities, so the phrase "or entity" in the definition of third party is unnecessary. Accordingly,

the final rule defines third party to mean any person that is not the consumer about whom the covered data pertains or the data provider that controls or possesses the consumer's covered data.

As discussed above in connection with the definitions of authorized third party and data aggregator, an entity may play different roles in different transactions and may serve as a data provider in one transaction and a third party in another transaction. The definitions are intended to identify what roles the parties are playing in a particular request for access to covered data. The CFPB concludes that additional clarifications in the definitions are not necessary.

B. Subpart B—Making Covered Data Available

1. Overview

Disagreements around the data that should be available to consumers and authorized third parties have limited consumers' ability to use their data and imposed costs on data providers and third parties. Subpart B of part 1033 addresses these obstacles by establishing a framework for the general categories of data that must be made available, including specific data fields that have been significant sources of disagreement, and exceptions from these requirements. Subpart B also restates the general requirement in CFPA section 1033(a) for data providers to make covered data available in an electronic form usable by consumers and includes a prohibition against evasion.

2. Availability and anti-evasion (§ 1033.201)

General obligation (§ 1033.201(a)(1))

Consistent with the general obligation in CFPA section 1033(a), the CFPB proposed in § 1033.201(a) to require a data provider to make available to a consumer and an authorized third party, upon request, 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, in an electronic form usable by consumers and authorized third parties. It also stated that compliance with the requirements in §§ 1033.301 and 1033.311 is also required.

The CFPB received only a few comments addressing the restatement of the statutory obligation in proposed § 1033.201(a). Of those, none objected to it and some, including consumer advocates in particular, supported the restatement. They argued that specific regulatory provisions could become outdated as technology evolves and that restating data providers' general statutory obligation in part 1033 would help make clear that the general obligation to make consumers' data available to them and to their authorized third party representatives stands nonetheless. A few data provider commenters requested that the rule be explicit that the "electronic form" of covered data may differ as between the consumer interface and the developer interface.[57]

For the reasons discussed herein, the CFPB is finalizing its restatement of CFPA's section 1033(a) general statutory obligation as § 1033.201(a)(1). The CFPB has removed the proposed additional sentence that referred to §§ 1033.301 and 1033.311, as it is unnecessary to state here that data provider obligations under § 1033.201(a)(1) are in addition to the data provider obligations under other provisions of subparts B and C. (Final § 1033.201(a)(2), regarding anti-evasion, is discussed below.)

The restatement in § 1033.201(a)(1) of the general obligation under CFPA section 1033(a) to make covered data available establishes the core obligation of data providers in part 1033. This obligation is in addition to the other requirements established by part 1033. As commenters observed, technology and business practices will continue to evolve over time. As

[57] The CFPB also received comments requesting that it undertake a consumer education campaign to ensure that consumers are aware of their rights under CFPA section 1033. While the CFPB continues to consider these suggestions, they are outside the scope of this rulemaking and the CFPB does not address them here.

they do, data providers' general statutory obligation to make covered data available will remain in place, implemented by § 1033.201(a)(1), as will data providers' obligations to comply with the other requirements of the rule set forth in subparts B and C of part 1033. To be clear, there may be overlap as to the substance of the requirements established by § 1033.201(a)(1) and the substance of the other requirements in subparts B and C, but that does not affect data providers' obligation to comply with the entirety of subparts B and C including § 1033.201(a)(1). There may also be obligations under § 1033.201(a)(1) that do not overlap with other requirements in subparts B and C; this likewise does not affect data providers' obligation to comply with § 1033.201(a)(1). Similarly, there may be requirements under the other provisions of subparts B and C that do not overlap with § 1033.201(a)(1); that does not affect data providers' obligation to comply with the other provisions of subparts B and C.

Under current industry practice, it is typical for the electronic form of data made available through data providers' consumer interfaces to differ from the electronic form of data made available through their developer interfaces. Nothing in § 1033.201(a)(1) or any other provision of part 1033 requires that aspect of current industry practice to change. Section 1033.201(a)(1) requires data providers to make covered data available in an electronic form usable by consumers and authorized third parties, but the electronic form usable by consumers need not be the same as the electronic form usable by authorized third parties.

Covered data in natural language

In the proposal, the CFPB stated that statutory requirement set forth in § 1033.201(a) that a data provider make available covered data in its control or possession obligates the data provider to make a consumer's covered data available in Spanish or English (or any other language) if that is the language in which the data provider maintains the consumer's covered

data. A few data provider commenters argued that the requirement should not apply to the developer interface.

That statement from the proposal remains an accurate description of data providers' obligations under § 1033.201(a); accordingly, the CFPB reaffirms it here. Some elements of covered data, discussed in more detail under § 1033.211, are non-numeric—that is, they include natural language. When a data provider controls or possesses covered data that includes natural language, the data provider must make available the data in the language in which the data provider controls or possesses the covered data (whether that language is Spanish, English, or any other language). Further, this obligation applies to both consumer and developer interfaces.

Anti-evasion provision (§ 1033.201(a)(2))

The CFPB requested comment on whether part 1033 should set forth an explicit prohibition against data provider conduct that would evade the objectives of CFPA section 1033, pursuant to the authority provided to the CFPB by CFPA section 1022(b)(1). More specifically, the CFPB requested comment on whether it should set forth explicit prohibitions against (1) actions that a data provider knows or should know are likely to interfere with a consumer's or authorized third party's ability to request covered data, or (2) making available information in a form or manner that a data provider knows or should know is likely to render the covered data unusable. The CFPB also requested comment on whether it should prohibit practices that might effectively make data unavailable or unusable to consumers and authorized third parties.

The CFPB received only a few comments addressing whether its final rule should include a prohibition against evasion. Data provider commenters that addressed the issue opposed such a prohibition on the grounds that it would be premature because actual evasive activity remains speculative. In contrast, third party commenters that addressed the issue supported inclusion of a

prohibition against evasion. These commenters asserted that the proposed rule did not do enough to prevent data providers from interfering with access, such as by varying the performance of their interfaces, by implementing systems in non-standard ways that limit interoperability, or by imposing excessive burdens or procedures that restrict or delay access to covered data depending on which third party is requesting access. They also asserted that there is a history of data provider efforts to delay or interfere with data access by authorized third parties.

The CFPB has determined that is necessary and appropriate to include in part 1033 a prohibition against evasion, pursuant to the CFPB's authority under CFPA section 1022(b)(1). Accordingly, the CFPB is adopting § 1033.201(a)(2) for the reasons discussed herein, which states that a data provider must not take any action (1) with the intent of evading the requirements of subparts B and C of part 1033; (2) that the data provider knows or should know is likely to render unusable the covered data that the data provider makes available; or (3) that the data provider knows or should know is likely to prevent, interfere with, or materially discourage a consumer or authorized third party from accessing covered data consistent with part 1033.

The anti-evasion provision in § 1033.201(a)(2) prohibits data provider conduct that is taken to evade the requirements of this final rule but which the CFPB may not, or could not, have fully anticipated in developing the rule. Part 1033 contains certain requirements that are targeted at potential data provider evasion and which rely in part on the CFPB's authority to prevent evasion under CFPA section 1022(b)(1). However, the CFPB cannot anticipate every possible way in which data providers might seek to evade the requirements of part 1033. The CFPB has determined that § 1033.201(a)(2) provides flexibility to address future data provider conduct taken to evade part 1033. The CFPB has also determined that the evasion prohibition will

enhance the effectiveness of the final rule's specific, substantive requirements, and thereby preserve the consumer rights provided by part 1033. In adopting the evasion prohibition, the CFPB's judgment is informed by concerns that commercial actors might be able to use their market power and incumbency to privilege their concerns and interests above fair competition that could benefit consumers.

Current data (§ 1033.201(b))

Proposal

In the facilitation of payment transactions, data providers regularly refresh covered data, and such data are often necessary to enable common beneficial use cases, like transaction-based underwriting and personal financial management. Both depository and nondepository data providers typically make available recently updated transaction and account balance data through online or mobile banking applications. However, the CFPB received questions during the SBREFA process about whether data providers could simply provide the last monthly statement rather than being required to make available recent transactions and current account balance. Proposed § 1033.201(b) interpreted CFPA section 1033(a) to require that, in complying with proposed § 1033.201(a), 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. It also specified that a data provider would need to make available information concerning authorized but not yet settled debit card transactions. The preamble discussed how this debit card transaction situation was an example and asked for comment on whether the provision regarding current data would benefit from additional examples or other clarifications.

When consumers make a request for information concerning a consumer financial product or service, the most recently updated information in a data provider's control or

possession is likely to be most usable. However, the proposal explained that § 1033.201(b) was not intended to limit a consumer's right to access historical covered data. The CFPB requested comment on whether the provision regarding current data would benefit from additional examples or other clarifications. The CFPB also requested input on issues in the market today with data providers making available only older information that is not fully responsive to a consumer's request.

Comments

Commenters did not object to a general requirement to make available the most recently updated covered data in the data provider's control or possession at the time of the request. One large data aggregator stated that the proposed data requirement is sufficiently clear, especially because it explains that pending transaction information must be made available. Some data provider commenters asserted that the CFPB should not require information concerning authorized but not yet settled debit card transactions. One data provider commenter stated that requiring pending transaction information is like asking financial institutions to look into a crystal ball to predict the future. The commenter asserted that some merchants, such as gas stations and hotels, send pre-authorizations for dollar amounts higher than the actual transaction amounts to ensure funds are available. Data provider commenters raised similar concerns about pending transaction information with regards to covered data under § 1033.211(a); those comments are discussed further below.

Final rule

For the reasons discussed herein, the CFPB is finalizing § 1033.201(b) as proposed with an edit to clarify the example of authorized but not yet settled transactions. The current data provision in § 1033.201(b) requires that, in complying with paragraph (a) of this section, a data

provider must make available the most recently updated covered data that it has in its control or possession at the time of a request. A data provider must make available information concerning authorized but not yet settled transactions. The CFPB notes that § 1033.201(b) does not limit a consumer's right to access historical covered data.

Finalizing this current data requirement helps ensure that data providers make available the most current data in their control or possession. Current data includes information regarding pending transactions that have not yet settled, including but not limited to pending debit card, credit card, and bill payment transactions. As discussed below with regards to transaction data in § 1033.211(a), pending transaction information can be helpful for a variety of use cases, including personal financial management. Although such information may ultimately change, consumers and third parties may need access to pending transaction information in order to plan for imminent withdrawals. Such information may also be necessary for a consumer or third party to determine whether a consumer needs to deposit additional funds into an account or is approaching a credit limit and thus should delay additional purchases. Data providers could limit funds or credit availability in response to pending transactions, and a consumer may need to know about pending transactions to understand any associated changes in available funds or credit. Given how authorized but not yet settled transactions may encompass a variety of payment types now and in the future, including credit card and certain bill pay transactions, and the risk that the debit card example might be misinterpreted to narrow the scope of this current data requirement, the final rule text removes the term "debit card" to more generally explain that a data provider must make available information concerning authorized but not yet settled transactions.

3. Covered data (§ 1033.211)

In general

Proposal

CFPA section 1033(a) generally requires data providers to make available, upon request, "information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data." The CFPB proposed in § 1033.211 to implement this by defining the information that a data provider would need to make available under the general obligation to make covered data available in proposed § 1033.201(a). Proposed § 1033.211 used the term covered data instead of the statutory term "information" and defined covered data to encompass several categories of information, as applicable: transaction information (including historical transaction information), account balance, information to initiate payment to or from a Regulation E account, terms and conditions, upcoming bill information, and basic account verification information.

The proposal explained that this covered data definition would leverage existing operational and legal infrastructure and that requiring data that are generally made available to consumers today would support most beneficial consumer use cases. The CFPB noted that certain proposed categories of data, such as upcoming bill information, historical transaction information, information to initiate a transfer to or from a Regulation E account, and basic account identity information can support account switching because it can ease the account opening process, identify recurring payments that need to be set up at the new account, and

transfer funds out of the old account. The CFPB requested comment on the benefits and data needs for consumers who are in the process of switching accounts.

The CFPB preliminarily concluded that the covered data definition also would address several issues in the consumer-authorized data sharing system today, including clarifying which data must be made available under the consumer's CFPA section 1033 right. Currently, data providers provide authorized third parties with inconsistent access to data. Pricing terms, like APR, have been particularly contested. Inconsistent access to consumer-authorized data may prevent the development of new use cases and the improvement of existing use cases. In addition, inconsistent access to consumer-authorized data may be hindering standardization in the market, and therefore further hindering competition and innovation, as parties must negotiate individual categories of information to be made available.

To address concerns about data providers restricting access to specific pieces of information, the proposed rule also gave examples of information that would fall within the covered data categories. The CFPB explained that these examples were illustrative and were not an exhaustive list of data that a data provider would be required to make available under the proposed rule. Under the proposed rule, a data provider would only have an obligation to make available applicable covered data; for example, a Regulation E financial institution providing only a Regulation E account would not need to make available a credit card APR or billing statement. The CFPB requested comment on whether additional data fields should be specified to minimize disputes about whether the information would fall within the covered data definition. The CFPB explained that, as proposed, the rule would allow flexibility as industry standards develop while minimizing ambiguity over the types of information that must be made available.

The CFPB also requested comment on whether the proposed categories of information provide sufficient flexibility to market participants to develop qualified industry standards.

The CFPB explained that these provisions would carry out the objectives of CFPA section 1033 of ensuring data are usable by consumers and authorized third parties by focusing on data that stakeholders report are valuable for third party use cases and that are generally under the control or possession of all covered persons. These provisions also would promote the use and development of standardized formats for carrying out the objectives of CFPA section 1033(d) by encouraging industry to focus format standardization efforts around these data categories.

Comments

Data providers, third parties, and other commenters generally supported the CFPB's categories and examples approach to defining covered data, noting that the categories-plus-examples approach allows market flexibility. Commenters also stated that the proposed categories of covered data would leverage existing legal and operational infrastructure, and that these covered data are generally available on consumer interfaces today. However, some commenters requested additional clarity or narrowing of the covered data categories, such as explaining that the covered data obligations only apply with regards to the covered consumer financial product or service. A few data provider commenters stated that the data categories should be narrowed significantly because they asserted that covering categories like pending transactions, terms and conditions, and upcoming bill information would exceed the CFPB's CFPA section 1033 authority. A few data provider commenters requested more specificity, such as defining all required data fields.

Some third party, consumer advocate, and other commenters requested that the CFPB expand the scope of covered data. For example, one consumer advocate commenter stated that covered data should include login usernames and passwords, challenge question responses, and customer service history. As another example, a third party commenter asked the CFPB to include a consumer identification number that could be linked to all consumer accounts, a consumer's date of birth, the date an account was opened, an account's transferability status, and other account status information. A large data aggregator asked the CFPB to specifically require data providers to provide the consumer's periodic statements as PDF documents. One commenter asked for clarification that, where a data provider is obligated to make available licensed information pursuant to the rule, the data provider does not provide a license to the authorized third party.

Final rule

For the reasons discussed herein, the CFPB is finalizing the proposed approach to covered data—that is, defining a list of categories of data that data providers must make available together with non-exhaustive examples of data fields that fall within those categories. The categories and examples approach to covered data appropriately balances resolving areas of market disagreement with avoiding detailed specifications, such as defining all individual data fields, that could interfere with efficiency and innovation.

The CFPB declines to expand the scope of covered data in this first rule to implement the substantive provisions of CFPA section 1033. The covered data definition in this final rule leverages existing operational and legal infrastructure: data providers generally make this covered data available through consumer interfaces, and existing laws require most of the categories of information to be disclosed through periodic statement and account disclosure

requirements. Requiring data that are generally made available to consumers today supports most beneficial consumer use cases, including transaction-based underwriting, payment credential verification, comparison shopping, account switching, and personal financial management. This covered data definition addresses several issues in the consumer-authorized data sharing system today, including (1) maximizing consumer benefits by clarifying which data must be made available under the consumer's CFPA section 1033 right; (2) addressing potential data provider anticompetitive conduct and incentives to withhold particular data fields; and (3) promoting conditions for standardization in the market. These covered data fall within the CFPB's authority under section 1033 as they are information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person. With respect to whether the data provider necessarily provides a license to authorized third parties to licensed information required to be made available under the rule, the rule does not require data providers to do so. Authorized third parties are subject to the limitations on collection, use, and retention under § 1033.421. At the same time, the rule requires covered data to be made available upon request, subject to the exceptions at § 1033.221, including an exception for confidential commercial information. The commenter did not specify what type of information might be subject to a license, but it is unlikely that the covered data defined at § 1033.211 would be subject to a license; and such information is generally made available to consumers today.

Comments received on the proposed categories and examples, and changes made in the final rule, are discussed below.

Transaction information (§ 1033.211(a))

The CFPB proposed in § 1033.211(a) to make available transaction information as covered data, providing examples of amount, date, payment type, pending or authorized status, payee or merchant name, rewards credits, and fees or finance charges. The CFPB explained that this category would refer to information about individual transactions, and discussed SBREFA feedback from bank data providers to exclude pending transactions. The CFPB preliminarily concluded that pending transaction information would support a variety of beneficial use cases.

The CFPB also proposed to include historical transaction information in the control or possession of the data provider. Proposed § 1033.211(a) explained that a data provider would be deemed to make available sufficient historical transaction information for purposes of § 1033.201(a) if it makes available at least 24 months of such information. The CFPB explained that historical transaction data supports a variety of use cases, including transaction-based underwriting, account switching, and personal financial management, but also observed that data providers do not make a consistent amount of historical transaction information available.

The CFPB discussed how many stakeholders, including third party small entity representatives during the SBREFA process, have provided feedback that 24 months of historical transaction data would support the vast majority of consumer use cases. Some data provider and consumer advocate stakeholders have explained that 24 months would be consistent with the recordkeeping requirements in Regulation E and Regulation Z. The CFPB preliminarily concluded that setting a safe harbor at a minimum of 24 months would ensure that consumers have access to sufficient historical transaction data for common beneficial use cases, while providing compliance certainty to data providers. This length of time would also be consistent with the existing recordkeeping timeframes in Regulation E, 12 CFR 1005.13, and Regulation Z,

12 CFR 1026.25. The CFPB also noted that data providers typically control or possess more than 24 months of historical transaction data and may continue to make more than 24 months available.

The CFPB requested comment on whether the transaction information examples were sufficiently detailed and consistent with market practices, whether to retain the safe harbor for historical transaction data, and whether a different amount of historical transaction data would be more appropriate. The CFPB also requested comment on whether and how the rule should require that data providers make available historical data for other categories of information, such as account terms and conditions, whether such historical data are kept in the ordinary course of business today, and the use cases for such data.

Comments

Commenters generally did not oppose inclusion of transaction information within the scope of covered data, with some data provider commenters asserting that this information is clearly required under CFPA section 1033. A few data provider commenters asked for additional clarification, such as whether the merchant name field refers to the merchant shown in the transaction description in the periodic statement or other sources like a web-based search about the merchant. Many data provider commenters opposed covering pending transaction information and reiterated concerns raised during the SBREFA process, including arguments that such information is not provided on monthly account statements, falls outside the CFPB's 1033 authority as it is not concerning a product that the consumer "obtained" from the data provider, is confusing for consumers, and could change at settlement so introduces error risk.

Some commenters opposed the rewards credits example, stating that this information is proprietary, difficult to disclose, subject to misinterpretation, not disclosed today, and could

erode the incentives of data providers to invest in merchant categorization tools. A few of these commenters asked the CFPB to limit the information to rewards balance, which they explained is typically made available today.

Third party commenters generally supported the 24-month safe harbor for historical transaction data, stating that 24 months would support most use cases and is consistent with market practices today. A consumer advocate commenter supported the consistency between this period and Regulation Z, 12 CFR 1026.25(a) and Regulation E, 12 CFR 1005.13(b), as both require retention of records for two years to document compliance with their requirements. One third party commenter asked the CFPB to require seven years of historical transaction data and a consumer advocate commenter suggested a period of three years. Some data provider commenters and SBA Advocacy recommended that the safe harbor should be narrowed to a shorter period, such as six or 12 months. A trade association representing data providers stated that the historical data provision would be inconsistent with section 1033(c), which states, "Nothing in [CFPA section 1033] shall be construed to impose any duty on a covered person to maintain or keep any information about a consumer." 12 U.S.C. 5533(c).

Final rule

For the reasons discussed herein, the CFPB is finalizing the transaction information requirement as proposed, including the requirement to provide historical transaction information and the 24-month safe harbor, with a minor edit to clarify that the example is referring to transaction date. The CFPB has determined that this pending transaction information is beneficial to consumers given how it supports use cases like personal financial management and fraud prevention, and is generally made available to consumers and third parties today. The CFPB has determined that a 24-month safe harbor period will support most use cases, will

encourage more consistent data access across institutions, is consistent with market practices today, aligns with existing record retention requirements in Regulation E and Regulation Z, and appropriately balances providing compliance certainty and encouraging standard market practices with allowing flexibility in case there are data providers who do not control or possess 24 months of historical transaction information notwithstanding their other regulatory obligations. A shorter safe harbor, such as 6 months, would not sufficiently support common use cases like personal financial management and loan underwriting, which typically require more historical transaction information and may be particularly reliant on more data when a consumer's income has seasonal variations. Given that data providers can determine how much historical transaction information to make available according to how much is in the data provider's control or possession rather than by taking advantage of this safe harbor, this provision is consistent with CFPA section 1033(c), which states that nothing in this section shall be construed to impose any duty on a covered person to maintain or keep any information about a consumer. However, the CFPB expects that data providers generally will have at least 24-months of historical transaction information in their control or possession given the existing Regulation E and Z record retention requirements.

Account balance (§ 1033.211(b))

The CFPB proposed in § 1033.211(b) to require data providers to make available account balance. The CFPB explained that in preamble that this category would include available funds in an asset account and any credit card balance. The CFPB requested comment on whether this term is sufficiently defined or whether additional examples of account balance, such as the remaining credit available on a credit card, are necessary.

A few data provider and third party commenters asked for specific clarifications related to account balance, such as stating that account balance means "current balance and statement balance," balance for credit cards means "total balance owed," and that the CFPB should require currency information. One data provider commenter requested that the CFPB require detailed account balance specifications based on payment type given differences in how various payment networks determine the available balance, ledger balance, and settlement.

For the reasons discussed herein, the CFPB is finalizing the requirement to provide account balance information as covered data. The CFPB has determined that account balance is not a commonly disputed category and that the market will benefit from flexibility in determining how to break down various account balances that apply to an account. However, the CFPB recognizes that a variety of account balances can apply to a product and use case—such as cash advance balance, statement balance, and current balance—and will monitor the market to ensure that data providers are making available this information in a manner usable by consumers and third parties.

Information to initiate payment to or from a Regulation E account (§ 1033.211(c))

In § 1033.211(c), the CFPB proposed to require a data provider to make available information to initiate a payment to or from the consumer's Regulation E account. An example would have explained that this category includes a tokenized account and routing number that can be used to initiate an ACH transaction. It also explained that a data provider would be permitted to make available a tokenized account and routing number instead of, or in addition to, a non-tokenized account and routing number.

The CFPB discussed how Regulation E account numbers are typically shared through consumer interfaces and are required to be disclosed under existing Regulation E periodic

statement provisions. Account numbers and routing numbers can be used to initiate a transfer of funds to or from a Regulation E account over the ACH network, enabling common use cases like initiating payments and depositing loan proceeds. Although data providers have recourse under private contracts, private network rules, and commercial law to recover funds stolen by an unauthorized entity, many data providers have expressed concern about their Regulation E obligations and urged the CFPB to allow the sharing of TANs with authorized third parties. The CFPB discussed how these TANs, which are in use today, may help mitigate fraud risks to consumers and data providers. TANs allow data providers to identify compromised points more easily and revoke payment credentials on a targeted basis (rather than issuing a new account number to the consumer). However, some third parties have asserted that TANs do not support certain use cases, such as allowing third parties to print checks to pay vendors, initiating payments by check or wire, and detecting fraud.

The CFPB preliminarily concluded that TANs allow third parties to enable most beneficial payment use cases while mitigating fraud risks, and therefore data providers should have the option of making TANs available to authorized third parties in lieu of full account and routing numbers. The CFPB noted that a TAN would only meet this requirement if it contained sufficient information to initiate payment to or from a Regulation E account. The CFPB requested comment on whether to allow TANs in lieu of non-tokenized account and routing numbers, including whether TANs would mitigate fraud risks and, in contrast, whether TANs have any limitations that could interfere with beneficial consumer use cases, and whether and how adoption and use of TANs might be informed by qualified industry standards. The CFPB also requested comment on whether data providers should also be required to make available information to initiate payments from a Regulation Z credit card.

Comments

Some data providers and trade associations opposed the proposed requirement to make available information to initiate payment to or from a Regulation E account, stating that sharing such information would introduce liability risks to data providers and consumers and asserting that payment initiation falls outside the CFPB's authority under CFPA section 1033. In contrast, a few other commenters stated that requiring account number would be appropriate and that they generally make this information available to consumers and third parties today. Some data provider commenters expressed their opposition to the growing usage of "pay-by-bank," a phrase sometimes used to describe consumer-to-merchant payment alternatives to the debit and credit card networks. These commenters asserted that the ACH network is not appropriate for third party payments and therefore the CFPB should not require data providers to make available ACH payment initiation information. One trade association representing bank data providers asked the CFPB to clarify that this category does not include the ability to of a third party to initiate credit-push payments from a consumer's account.

A few data provider commenters asked the CFPB to clarify the scope of the required information and whether account and routing number would satisfy the obligation. Data provider commenters also raised ambiguity and overbreadth concerns, asserting that this provision could be read to require wire transfer information and other payment information within the data provider's control or possession. Several data provider commenters opposed adding a requirement to make available information to initiate payment from a credit card account, asserting that requiring credit card number would introduce significant risks to consumers and data providers and that the CFPB had not sufficiently considered the risks of requiring such data. Some third party and data provider commenters stated that some account information is

necessary to allow consumers and third parties to differentiate accounts, including situations where a consumer needs to identify which account they are permissioning access to, or when a third party is verifying a consumer's assets for loan underwriting.

Many third party commenters supported including information to initiate payment, with some asking the CFPB to clarify that it includes other payment types beyond ACH. For example, one data provider commenter that is also a third party asserted that the category should be expanded to include all means to initiate payments, including debit card information and FedNow information.

The CFPB received mixed comments on the allowance for TANs. Although some data providers focused their comments on concerns related to providing payment initiation information generally, others noted the potential security benefits of TANs and supported the proposed approach. Commenters supporting use of TANs stated that they enable data providers to identify the point of compromise in case of a breach; enable consumers and data providers to revoke compromised payment credentials on a targeted basis; enable data providers and consumers to limit risks of bank account fraud, as they can be restricted to a particular third party; and offer simple implementation and reliable technology given that they exist in the market today and can be easily adopted. One commenter stated that TANs would allow a data provider to create a token for a specific third party, so that any transactions on that token can be attributed to the third party. Commenters also stated that consumers can more easily revoke TANs when a payee is misusing the token or the consumer otherwise wants to revoke authorization, rather than needing to completely close an account and disrupt other account payment activity. Tokens also enable data providers to better identify the source of a cybersecurity incident or fraud, and would allow data providers to quickly stop fraud on a

compromised token by restricting the ability to transact with that token. One large data aggregator stated that allowing TANs in lieu of non-tokenized account numbers could encourage further development of pay-by-bank functionality. This commenter also requested several significant modifications to the TAN option, such as allowing the third party to obtain the non-tokenized account and routing number if a TAN does not meet the third party's particular use case, and requiring data providers who share a TAN to also make available a unique user identifier. A payment network governance organization supporting TANs stated that industry does not tokenize routing numbers.

Some third parties opposed allowing data providers to make available TANs in lieu of non-tokenized account and routing numbers as proposed. These commenters asked the CFPB to remove the allowance for TANs and only allow non-tokenized account and routing numbers, asserting that the ability to revoke TANs introduces risks of fraud perpetrated by consumers, TAN payments are more likely to fail, there is potential for data providers to issue TANs in an anticompetitive manner, TANs should be addressed in a separate rulemaking, and TANs do not support some consumer and third party use cases like generating paper checks, assessing the likelihood of payment failure, and interfering with fraud controls that track a particular account's payment activity. A few third parties also asserted that there is no market-wide standard for TANs and that TANs are not interoperable among the payment networks used today, including FedNow, Real-Time Payments (RTP), and ACH. These commenters differed on whether it would be appropriate to defer to a standard setting organization to determine the specifications for TANs. Some shared concerns that if the CFPB finalized the TAN option, the rule should adopt specific TAN revocation and expiration provisions. One trade association commenter and a third party commenter stated that non-tokenized account and routing number information is not

that sensitive because it is printed on paper checks and already needs to be encrypted according to private network rules. A third party commenter asserted that industry-wide controls serve as better protective tools than optional use of TANs, as the ACH network already monitors for high returns rates in order to identify fraudsters running unauthorized debits against stolen ACH numbers, banks who sponsor third party senders into the ACH system are required to perform due diligence on those senders, consumers have rights under Regulation E to have their bank reverse an unauthorized payment, and banks regularly honor consumer claims of unauthorized account activity even if there is no evidence that the account activity was unauthorized.

Final rule

For the reasons discussed herein, the CFPB is finalizing the § 1033.211(c) category of information to initiate payment to or from a Regulation E account, including language allowing data providers to make available TANs in lieu of non-tokenized account numbers, with some clarifications.

The CFPB has determined that information to initiate payment to or from a Regulation E account supports many essential consumer use cases such as account switching and making payments. The CFPB understands that consumers use account and routing numbers today to support use cases like signing up for direct deposit, making bill payments, and designating an account to accept loan proceeds. Consumers can provide this information directly to third parties, but making it available through a data provider has a variety of benefits, including accuracy of the number sequence, ensuring that a correct and valid account is being accessed, and reduced friction in how quickly and easily that information shared. This information falls within the CFPB's authority under section 1033 as it is information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained

from such covered person. As discussed above in part IV.3, the rule does not require account write access or otherwise require payment initiation. Part IV.3 includes additional discussion of comments related to concerns about liability.

Some data provider and trade association commenters asked the CFPB to clarify that pre-existing payment authorization requirements continue to apply. The CFPB agrees with commenters that regardless of whether a third party obtains information to initiate payment from a consumer or from an authorized third party, that third party would need to obtain appropriate payment authorization from the consumer. If the third party is not a depository institution, it would need to go through an originating depository institution to access the ACH payment network, and that originating depository institution continues to have due diligence, Know-Your-Customer, and private network obligations in terms of warranting that the third party's payment order is valid. The consumer's receiving depository financial institution and any other financial institutions in the transaction would also have Regulation E obligations, including error resolution obligations for any unauthorized payments. However, according to private network rules, the receiving depository financial institution can seek remediation for errors from the originating depository financial institution and third party that facilitate the erroneous payment.

Given the benefits of making this information available, how it is required to be disclosed under Regulation E periodic statement requirements, how it is generally made available to consumers and third parties today, applicable Regulation E error protections for consumers in the event the information is misused, existing private network and safety and soundness obligations of originating depository institutions that facilitate a third party's payment, and the ability of the depository data providers to seek redress from originating depository institutions for erroneous

payments, the CFPB has determined that data providers must make available information to initiate payment to or from a Regulation E account held by the data provider.

Instead of using the term "account and routing number" to define this covered data category, the CFPB is finalizing the broader proposed "information to initiate payment" language for two forward-looking reasons. First, the payments market may start to shift away from account and routing number as security and data practices evolve, and this broader language provides the market with flexibility to share data in accordance with those shifts. Second, since third parties typically use account and routing number to complete ACH payments today, using the "account and routing number" term may be misinterpreted to limit the types of payments that the information can be used to initiate. As the payment market evolves and more broadly adopts alternatives to the ACH network, such as RTP and FedNow, data providers may control or possess other payment initiation information that can be retrieved in the ordinary course of business—and accordingly such information would need to be made available. This information could include information sufficient to submit a request for payment. However, this provision is limited to information sharing and accordingly does not include the ability of a third party to access and push payment out of a consumer's account, also referred to as "write" access.

To clarify the scope of this information and address commenters' concerns about ambiguity, the CFPB is finalizing a clarification that this category is limited to information to initiate payment to or from a Regulation E account held directly or indirectly by the data provider. The final rule also explains that the requirement to make available this information does not apply to data providers who do not directly or indirectly hold the underlying Regulation E account. For example, a data provider that merely facilitates pass-through

payments to third parties would not be required to make available account and routing number for the underlying Regulation E account.

The CFPB notes that CFPA section 1033(b)(4) and the final rule at §§ 1033.211(c) and 1033.221(d) only require data providers to share payment initiation information that they can retrieve in the ordinary course of business. In the current market, account number is clearly retrievable in the ordinary course of business given that it is typically shared through consumer and developer interfaces today and is required to be disclosed on the Regulation E periodic statement. The CFPB is not requiring payment initiation information that is not retrievable in the ordinary course of business. For purposes of this rule, the CFPB is making the determination that debit card numbers are data that are not retrievable in the ordinary course because of a unique historically-driven combination of factors that together suffice to put this data outside the scope of the rule, including the physical way—plastic cards—in which providers have typically chosen to make debit card credentials available to consumers, and the specific nature of how longstanding private payment network rules govern which entities can issue and control debit card payment credentials. As noted above, as the payment market adopts alternatives to the ACH network, such as RTP and FedNow, data providers may control or possess other payment initiation information that data providers can retrieve in the ordinary course of business—and accordingly such information would need to be made available.

This provision does not impact other requirements for initiating payment or accessing the payment networks. Section 1033.211(c) requires that data providers make available information to initiate payment to or from a Regulation E account; payment authorization requirements continue to separately apply. The CFPB confirms that, in order to initiate payment, third parties would need proper payment authorization from the consumer subject to, without limitation,

Regulation E preauthorized electronic fund transfer provisions and private network rule authorization requirements. The CFPB notes that, in order to access the payment network and initiate an ACH or similar payment, a third party would need an originating depository financial institution relationship. With regards to payment initiation, this provision does not alter due diligence and network requirements that apply to originating depository financial institutions providing access to the ACH payment network.

The CFPB is also finalizing, with modifications, the proposed example that would allow data providers to share a tokenized account number instead of, or in addition to, a non-tokenized account number. This clarification is now moved into the rule text paragraph and no longer is labeled as an example. To address commenters' concerns about anticompetitive issuance of TANs, the rule text also now states that such tokenization is appropriate so long as it is not used as a pretext to restrict competitive-use of payment initiation information; the reference to "routing number" has been removed in light of comments that routing number is not typically tokenized. TANs, used appropriately, can meet consumer use cases for electronic payments. The CFPB notes that use of TANs in conformance with applicable consensus standards can serve to indicate appropriate use. In addition, data providers have legitimate reasons to use TANs because they can protect the security of the relevant payment system and thus benefit its participants, including the consumer. In particular, TANs lower the risk of unauthorized transactions by limiting the potential for payment credentials to be misused for purposes the consumer did not intend or authorize, by helping to identify the source of a data breach, and by causing less disruption to consumers and the payment system when a credential is appropriately replaced. These benefits apply even though non-tokenized account numbers appear on paper checks and may need to be stored in an encrypted form according to private network rules. The CFPB notes

that a data provider's provision of a TAN in lieu of non-tokenized account number is optional and that sometimes consumers share non-tokenized account and routing numbers directly with third parties.

With regard to concerns from some third party commenters that TANs can interfere with fraud controls that track an account's payment history, third parties can use the account identifier described under § 1033.211(f) to distinguish consumer accounts. However, the CFPB cautions that § 1033.421(a) limits authorized third party use of covered data, including TANs, to what is reasonably necessary to provide the consumer's requested product or service. The general limitation standard, including uses that are reasonably necessary to protect against actual or potential fraud, is discussed below regarding § 1033.421(a) and (c). TANs do allow consumers to more easily revoke their payment authorizations, but ease of revocation is a consumer benefit of TANs as it allows consumers to exercise more precise and immediate control over their account in the event that they have concerns about a payee. The interaction between TANs and revocation is discussed further in § 1033.331(e). In response to a third party commenter's statement that industry controls are more effective than TANs, the CFPB notes that unauthorized payment fraud exists in the market today and the CFPB has taken public action against financial institutions that do not comply with their error resolution requirements.

This final rule does not require data providers to grant access to, or facilitate payments on, any particular payment network. Accordingly, the CFPB does not require that TANs be interoperable across multiple payment networks. However, to the extent that data providers pretextually use TANs to frustrate consumers' ability to provide functioning payment initiation information to authorized third parties of their choice, such pretextual use would violate the anti-evasion provision at § 1033.201(a)(2). The CFPB intends to monitor the market for any such

pretextual use of the allowance for TANs, and will issue future guidance about the use of TANs in lieu of a full account number if needed.

Terms and conditions (§ 1033.211(d))

The CFPB proposed to require terms and conditions be made available as covered data in § 1033.211(d). The CFPB explained that terms and conditions generally refer to the contractual terms under which a data provider provides a covered consumer financial product or service. The proposed rule included several non-exhaustive examples of information that would constitute terms and conditions.

The CFPB discussed how certain terms and conditions, such as pricing, reward programs terms, and whether an arbitration agreement applies to the product, support beneficial use cases, like comparison shopping and personal financial management. Authorized third parties could use this information to help consumers more easily understand and compare the terms applicable to a covered consumer financial product or service. Since pricing is a fundamental term that is provided in account opening disclosures and change in terms disclosures, the CFPB proposed to include APR, APY, fees, and other pricing information in this category. The CFPB also discussed how this provision would benefit consumers because they may not be able to easily find this information through a consumer interface today, and some data providers may not be consistently sharing it with third parties. The CFPB requested comment on whether the final rule should include more examples of information that must be made available under terms and conditions.

Comments

Data provider commenters generally did not dispute including APR and APY as examples of covered data, although a few opposed sharing that information. Some bank data

provider and related trade association commenters opposed including information other than realized fees, such as applicable fee schedule. Some data provider commenters opposed including other examples in the final rule, such as rewards program terms, overdraft opt-in status, and whether an account was subject to an arbitration agreement, arguing that such information falls within the exceptions in § 1033.221 or otherwise falls outside the CFPB's 1033 authority as it is not related to the covered consumer financial product or service and is not cost, charges, or usage data. One credit union trade association stated that arbitration information will make consumers targets for predatory attorneys and contradicts statements in a separate CFPB rulemaking regarding covered form contracts used by nonbanks.

Many data provider commenters raised technical and burden concerns about this category, stating that terms and conditions are not well suited to developer interfaces, as some terms cannot be reduced to numerical or binary data fields. Other stated concerns included: (1) lack of clarity over whether the rule is requiring a PDF of an entire terms and conditions document; (2) the number of terms and conditions documents applicable to an account, and whether all of them must be made available; (3) full terms and conditions documents are not useful or desirable for third parties to receive; (4) sharing full terms and conditions documents entails sharing of extraneous information; and (5) sharing current terms and conditions documents is overly burdensome and infeasible. A data aggregator commenter asserted that full terms and conditions contain some substantial legal terms that are neither supportive of any existing use cases nor easily transformed into a machine-readable format. This commenter requested that the CFPB identify the data elements that may be maintained in the terms and conditions and require that those elements—rather than the full terms and conditions—be made available in a machine-readable format.

One bank trade association commenter asked the CFPB to allow data providers to share a PDF of the complete terms and conditions rather than through data fields, and another suggested allowing data providers to post terms on their website rather than making them available through the developer portal. A large data aggregator commenter explained that some third party interfaces allow PDF documents to be shared today.

Final rule

For the reasons discussed herein, the CFPB is finalizing the requirement to make available terms and conditions as covered data, with some additional limitations. The CFPB is aware that a variety of terms and conditions may impact a covered consumer financial product or service and some of those terms may not support current consumer use cases. The CFPB agrees with commenters that terms and conditions can be defined to provide compliance clarity to data providers and limit the extent of information they need to make available, while supporting current and potential use cases. Accordingly, the CFPB is finalizing a definition of the terms and conditions category limited to data in agreements evidencing the terms of the legal obligation between a data provider and a consumer for a covered consumer financial product or service, such as data in the account opening agreement and any amendments or additions to that agreement, including pricing information.

The CFPB has determined that the proposed non-exhaustive examples of terms and conditions are helpful to clarify the terms and conditions category and minimize market disagreements about whether certain pieces of information must be made available. The applicable fee schedule is important information for comparison shopping and personal financial management as consumers need to anticipate what fees can be charged in order to evaluate a product's true cost and plan spending. Rewards programs are an important factor to a consumer's

decision to obtain and use a consumer financial product or service, and the CFPB has determined that it is appropriate to require that these rewards program terms be made available under § 1033.201(a)(1). Similarly, whether a consumer has opted into overdraft coverage or is subject to an arbitration agreement is relevant to how a consumer may decide to use or comparison shop for a product or service, including determining applicable fees and their rights with respect to that product or service. All of these non-exhaustive examples reflect the terms and conditions of the legal obligation between a data provider and a consumer for a covered consumer financial product or service. In response to a comment that arbitration information will be used to target consumers or otherwise relates to other CFPB policies related to form contracts, this information is not being collected by the CFPB and will not be shared unless the consumer chooses to do so.

The CFPB has added credit limit to the list of non-exhaustive examples of terms and conditions. Credit limit is a key term that is typically determined and disclosed when a consumer obtains a Regulation Z credit card, and account agreements generally permit the provider to make changes to the credit limit. Although the CFPB asked for comment on credit availability with regard to account balance in § 1033.211(b), the CFPB has determined that it would be clearer to include credit limit as an example under this terms and conditions category. The CFPB is finalizing example 1 to § 1033.211(d) to state that this category includes the applicable fee schedule, any APR or APY, credit limit, rewards program terms, whether a consumer has opted into overdraft coverage, and whether a consumer has entered into an arbitration agreement.

In the current market, certain terms and conditions are commonly requested and made available as discrete data fields in developer interfaces. For example, discrete data fields for applicable APRs and APYs are typically shared in third party interfaces to support comparison shopping and personal account management. The CFPB expects that such commonly requested

terms and conditions will continue to be made available as discrete callable data fields, as § 1033.311 requires developer interfaces to make data available in a standardized and machine-readable format that is widely used by other data providers and designed to be readily usable by authorized third parties.

As use cases develop, third parties may seek access to terms and conditions that are not commonly used today. For example, a third party may need a specific term from the account opening agreement to provide a product or service requested by the consumer. If that term falls within terms and conditions as defined in § 1033.211(d), the term is covered data and the provider's developer interface must make that data available. However, the data provider's developer interface would not necessarily need to make that specific term available as a discrete "callable" data field. Instead, it could make it available within a broader section of the agreement or by making available the full account opening agreement, subject to the standardized and machine-readable format requirements in § 1033.311(b). As discussed in § 1033.421(b), the general limitation on use and retention of covered data in § 1033.421(a) would apply to that data. The CFPB concludes that given how some account agreement terms are not translatable to discrete numerical or binary data fields, it is appropriate for data providers to have flexibility in how they share terms and conditions information through the developer interface in a machine-readable format. (See part IV.C.2 for a discussion of the machine-readability requirement applicable to the developer interface.) Some data providers already appear to be sharing longer documents, such as statements, through developer interfaces today.[58] The CFPB also concludes that because (1) most account agreement terms are publicly available, broadly applicable and not specific to a particular consumer, and (2) third parties are restricted in terms of what information

[58] *See, e.g.*, Plaid, *Statements*, https://plaid.com/docs/statements/ (last visited Oct. 16, 2024).

they can use and retain under § 1033.421(a), the privacy concerns are limited in this particular situation.

Upcoming bill information (§ 1033.211(e))

The CFPB proposed in § 1033.211(e) to require upcoming bill information to be made available as covered data. An example explained that upcoming bill information would include information about third party bill payments scheduled through the data provider and any upcoming payments due from the consumer to the data provider. For example, it would include the minimum amount due on the data provider's credit card billing statement, or a utility payment scheduled through a depository institution's online bill payment service. The CFPB preliminarily concluded that this information would be necessary to support personal financial management and consumers who are switching accounts. The CFPB requested comment on whether this category was sufficiently detailed to support situations where a consumer is trying to switch recurring bill payments to a new asset account, such as transferring a monthly credit card payment to a new bank.

Comments

Some data provider commenters stated that upcoming bill information should not be included or should be significantly narrowed. These commenters asserted that this information is outside the CFPB's section 1033 statutory authority, is burdensome to collect and share, is unrelated to the covered consumer financial product or service, is sensitive because it contains payee data, is subject to change, and would not support account switching. A few data providers stated that it is unclear whether this information also includes payments scheduled through a third party, rather than being limited to bill payments scheduled through the data provider's platform. One data provider commenter stated that this information should be excluded as

confidential commercial information because contracts with billers and bill service provider prohibit its disclosure. One commenter stated that this information should be limited to bills related to financial products, like mortgage bills.

Final rule

For the reasons discussed herein, the CFPB is finalizing this provision as proposed, including the example discussing information about third party bill payments scheduled through the data provider and any upcoming payments due from the consumer to the data provider. Upcoming bill information will support several important consumer use cases, including personal financial management and account switching. In response to comments regarding whether payments scheduled through a third party are also meant to be covered, the CFPB confirms that data providers are not required to make available information that is not in the control or possession of the data provider, and upcoming bill payments scheduled outside of the data provider's bill payment platform may not be in their control or possession and thus are not considered covered data. For example, when a consumer uses a cell phone company's website to schedule a bill payment from their bank account, the consumer's bank may not control or possess that information unless the cell phone company is sharing that preauthorization information with the bank. In contrast, a bank does control or possess information about a cell phone payment a consumer scheduled through the bank's consumer interface, and so is required to make available that bill payment information under § 1033.201(a)(1). Contrary to commenters' assertions about the scope of the data access right, information about scheduled bill payments is squarely within the scope of CFPA section 1033(a); specifically, upcoming bill payments relate directly to a "series of transactions"—*i.e.*, the consumer's pattern of paying bills through the data provider. As discussed in the context of the general limitation standard in subpart D, third parties will be

limited to collecting, using, and retaining covered data only to the extent it is reasonably necessary to provide the consumer's requested product or service, and therefore sharing of covered data will be limited to what is reasonably necessary. The CFPB notes that the general exceptions under CFPA section 1033(b) continue to apply, subject to the anti-evasion provision in § 1033.201(a)(2).

Basic account verification information (§ 1033.211(f))

The CFPB proposed in § 1033.211(f) to require basic account verification information be made available as covered data, which would be limited to the name, address, email address, and phone number associated with the covered consumer financial product or service.

The CFPB discussed how certain pieces of identifying consumer information are commonly shared with third parties today to support several beneficial use cases. For example, a lender may seek to verify that loan disbursements will be deposited into an account that belongs to the consumer who is applying for the loan, or a mortgage underwriter may seek to verify that funds in a savings account belong to the mortgage applicant. On the other hand, third parties have raised concerns during the SBREFA process that data providers sometimes limit access to this information, and requested that the CFPB require that account verification information be shared.

The CFPB preliminarily concluded that requiring data providers to share basic account verification information is necessary to ensure the usability of the covered data. For example, confirming that funds in a savings account do, in fact, belong to the consumer applying for a mortgage loan is necessary to determine whether the mortgage underwriter can rely on that information. Similarly, a loan provider is mitigating fraud risks when it ensures that the name, address, email address, and phone number on a recipient account matches the information of the

loan applicant; matching information helps ensure that the funds are going to the correct account, and that the account opening notifications are not going to someone who stole the consumer's identity. Email addresses and phone numbers are increasingly being used as substitutes for consumer and account identifiers, particularly in the payments market where such information can be used to send a person-to-person payment. Accordingly, the CFPB preliminarily determined that limiting basic account verification information to the name, address, email address, and phone number associated with the covered consumer financial product or service would facilitate the most common use cases and is consistent with market practices today.

The CFPB considered whether to include SSNs as part of basic account verification information, as SSNs are shared for some beneficial consumer use cases, like mortgage underwriting. However, the sharing of SSNs is not ubiquitous. The CFPB preliminarily concluded that SSNs may continue to be shared as appropriate but, given the risks to consumers, the proposed rule did not require data providers to make them available.

The CFPB requested comment on whether the proposed basic account verification information category would accommodate or unduly interfere with beneficial consumer use cases. Given privacy and security concerns about unintentionally covering other kinds of information that are not typically shared today, the CFPB also requested comment on whether it is appropriate to limit this category to only a few specific pieces of information.

Comments

Both consumer advocate and bank data providers generally supported the CFPB's approach to allowing some basic account verification information but limiting the category to specified data fields. These commenters agreed that this approach would appropriately balance supporting common beneficial use cases with limiting consumer privacy risks and data provider

implementation costs. Many of these commenters also specifically requested that the CFPB not expand the category to include SSN or other personally identifiable information. A trade association representing data providers asked that the CFPB not expand this category to any information a data provider uses to securely authenticate the identity of its customer as part of a payment initiation process, such as a one-time verification code, as such information would pose significant risks to the integrity of various payment security standards and would conflict with the FFIEC's guidance on Authentication and Access to Financial Institution Services and Systems. Some data provider commenters opposed sharing any basic account verification information, asserting that such information presents fraud risks, has no benefit, and can be obtained directly from consumers. A trade association representing large depository data providers stated that additional account information could help consumers identify which account data they would like to share. This commenter asserted that the CFPB could add "number of the account" to this category, with an allowance for use of tokens or truncated account numbers, and that it is common practice today for truncated account numbers to be used for this purpose. A third party commenter stated that account identification is necessary for underwriting so that a third party knows whether a consumer's assets have already been accounted for. Another third party commenter asked the CFPB to include a consumer identification number that could be linked to all consumer accounts, a consumer's date of birth, the date an account was opened, an account's transferability status, and other account status information.

Final rule

For the reasons discussed herein, the CFPB is finalizing basic account verification information as proposed, with the addition of certain account-identifier information for situations where a data provider directly or indirectly holds a Regulation E or Regulation Z account.

The CFPB has determined that this approach sufficiently enables beneficial consumer use cases in the market today and avoids introducing risks from adding account verification information that is not commonly made available. The information specified in § 1033.211(f) supports a variety of use cases and thus is appropriate to require, including ensuring that loan proceeds are being deposited into an account belonging to the consumer, confirming that the consumer applying for credit does hold the asset accounts being used for underwriting, and reducing friction during account opening. In order to verify an account, third parties often need to match the information provided by the consumer with the identification information held by the data provider. Consumers and third parties may need to identify an account in order to permission access and differentiate a consumer's assets.

In response to comments about the need to differentiate accounts, the CFPB is adding language to require that if a data provider directly or indirectly holds a Regulation E or Regulation Z account belonging to the consumer, the data provider must also make available a truncated account number or other identifier for that account. Given the more sensitive nature of other personally identifiable information requested by some commenters, such as SSN, at this time the CFPB is limiting this category to name, address, email address, and phone number associated with the covered consumer financial product or service, and, as applicable, account identifier. Data providers are permitted to provide additional information as appropriate and the

CFPB will monitor whether to expand the scope of required information as account verification practices evolve.

4. Exceptions (§ 1033.221)

Proposal

The CFPB proposed, in § 1033.221, four exceptions to the requirement that data providers make data available under the proposed rule, along with some clarifications of data that do not fall within these exceptions. The exceptions would implement section 1033(b) of the CFPA by restating the statutory language and providing certain interpretations. The first exception was for any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors. Some data providers have asserted that certain account information falls within this statutory exception because such information is an input or output to a proprietary model. The CFPB proposed to clarify that such information would not qualify for this exception merely because it is an input to, or an output of, an algorithm, risk score, or predictor. For example, APR and other pricing information are sometimes determined by an internal algorithm or predictor, but such information would not fall within this exception.

The second exception was for any information collected by a data provider for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct. During the SBREFA process, a third party stated that at least one data provider has cited this exception when declining to provide general account information, such as the name on the account. To avoid misuse of this exception where information has multiple applications, the CFPB proposed to clarify that information collected

for other purposes does not fall within this exception. For example, name and other basic account verification information would not fall within this exception.

The third exception was for information required to be kept confidential by any other provision of law. Information would not qualify for this exception merely because the data provider must protect it for the benefit of the consumer. The proposed example to this exception stated that the data provider cannot restrict access to the consumer's own information merely because that information is subject to privacy protections.

The final exception was for any information that a data provider cannot retrieve in the ordinary course of its business with respect to that information.

The CFPB explained that the definition of covered data in § 1033.211 would generally include information made available to consumers and authorized third parties today or that is required to be disclosed under other laws. The CFPB noted that the exceptions proposed in § 1033.221 were narrow, and the information specified as covered data would not typically qualify for any of these exceptions.

The CFPB requested comment on whether it should include additional examples of data that would or would not fall within the exceptions, and whether this provision sufficiently mitigates concerns that data providers may cite these exceptions on a pretextual basis.

Comments

Comments on the exceptions took a variety of positions. With respect to the CFPB's implementation of the statutory exceptions overall, some data provider and related trade association commenters asked the CFPB to add more examples of excepted information and expand the exception provisions. These commenters stated that the statutory exceptions should be interpreted broadly to allow data providers discretion in denying access to covered data. One

commenter stated that it is premature to have concerns about data provider abuse of the exceptions. A bank trade association commenter asked the CFPB to except any data that is not available in the consumer interface, explaining that such data pose an undue burden on financial institutions and introduce data security risks and operational challenges. In contrast, many third party commenters asserted that the CFPB should interpret the exceptions narrowly as they are vulnerable to pretextual use by data providers. One large bank trade association commenter asked the CFPB to finalize the exceptions as exemptions to make clear that data described under the statutory exceptions are not covered by the rule.

On the first proposed exception for confidential commercial information, many data provider commenters asserted that rewards programs terms and credits are proprietary and should fall under this exception, and that the rule should prohibit reverse engineering. A large data aggregator also requested that the rule prohibit reverse engineering of confidential commercial information, suggesting that such a prohibition could be incorporated into the data privacy protections. A trade association representing data providers asked that the CFPB distinguish between data that might be useful for a consumer for consumer purposes versus data that would be of primarily commercial value (such as metadata regarding the exact time and place of transactions), and stated that data providers should not be required to reveal analytically enriched data if the consumer does not ordinarily see such data and cannot be said to substantially rely upon it when making decisions about the selection of consumer products or services. This commenter asserted that the exception must make clear that it also extends to information that cannot be shared for contractual reasons and attorney work product related to an account and any active litigation.

A large data aggregator commenter supported the proposed examples for the first exception as sufficient and appropriate, stating that the proposed clarification that the exception for proprietary algorithms only applies to the algorithm itself, and not to the covered data that goes into or is an output from the algorithm, appropriately balances a data provider's right to protect its trade secrets and intellectual property with a consumer's right to data access and portability. Absent this clarification, the commenter cautioned that the exception could swallow the rule, explaining that today myriad terms, conditions, rates, fees, and features of an account are the result of some proprietary algorithmic decision making by the financial institution. A few consumer advocate commenters asked the CFPB to narrow this exception to clarify that credit scores and other risk scores are not considered confidential commercial information, and therefore must be made available.

On the second proposed exception for any information collected by a data provider for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct, a bank trade association commenter asserted that it was too narrow and should be revised to remove the term "sole." This commenter explained that very limited information is collected solely for fraud prevention. Another data provider trade association offered examples of information it believes fall within the statutory exception, such as information related to security incidents and internal account flags, and requested that the CFPB reconsider its approach to this exception.

On the third exception for information required to be kept confidential by any other provision of law, a few data provider commenters requested that the exception be expanded. One asked for examples of laws that would require a data provider to withhold information from a consumer, and a few urged the CFPB to add a good faith compliance standard for data providers

to withhold information if they reasonably believe that the information must be kept confidential by law.

On the fourth exception regarding information that a data provider cannot retrieve in the ordinary course of its business, one research institute commenter requested that it be narrowed as it may allow data providers to find loopholes or shield themselves from disclosing information that they should be required to provide to consumers. A data aggregator commenter requested changes so that data providers cannot evade their obligations to provide covered data by deliberately making it difficult to retrieve data in the ordinary course of business. The commenter suggested adding a presumption that all covered data are retrievable in the ordinary course at least for a period stretching from the present back at least 24 months and adopt an interpretation of the phrase "in the ordinary course" that relies on an objective industry standard and would not permit a data provider to adopt an unreasonable policy to evade data access obligations. A data provider commenter asked the CFPB to add examples of information that are within the scope of this exception, explaining that it believes terms and conditions and payments scheduled through third parties would be excepted. Another data provider commenter stated that 24 months of historical transaction data are not retrievable in the ordinary course of business, and that a shorter safe harbor of six months would be more appropriate.

One Member of Congress commenter cited the discussion in the proposal of how the exceptions proposed in § 1033.221 are narrow and that proposed § 1033.351(b)(1) would require a data provider to create a record of what covered data are not made available pursuant to an exception in proposed § 1033.221 and explain why the exception applies. This commenter asserted that proposed § 1033.221 and the interaction with proposed § 1033.351(b)(1) will ensure that consumer data are not withheld for anticompetitive reasons.

Final rule

For the reasons discussed herein, the CFPB is finalizing the exceptions, including the examples of data that do not fall within the exceptions, as proposed. The CFPB has concluded that additional examples of information that fall within the exceptions, as requested by some commenters, are not necessary at this time. The CFPB intends to monitor the market for pretextual use of the CFPA section 1033 exceptions and more generally for violations of the prohibition against evasion in § 1033.201(a)(2).With respect to a commenter's request to use rulemaking authority to reclassify the statutory term "exceptions" to "exemptions," the commenter did not explain why this change from the statute was necessary to clarify that these data types are not covered by the rule. The CFPB is thus finalizing the heading for § 1033.221 using the statutory language.

Confidential commercial information

Final § 1033.221(a) restates the exception at section 1033(b)(1) for any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors. Final § 1033.221(a) further clarifies that information does not qualify for this exception merely because it is an input to, or an output of, an algorithm, risk score, or predictor. Final § 1033.221(a) includes an example of APR and other pricing terms as data that are sometimes determined by an internal algorithm or predictor but do not fall within this exception.

With respect to comments that rewards programs terms, rewards credits, and terms and conditions are proprietary and should fall under the first exception for confidential commercial information, the CFPB has determined that these data do not fall within the definition of confidential commercial information. Today, rewards program terms are a factor in how consumers decide to use and select credit cards. They concern the covered consumer financial

product or service obtained from the data provider, and they support important consumer use cases like comparison shopping, personal financial management, and account switching. These terms are commonly shared with consumers, just like general terms and conditions for an account—similarly, the credits that a consumer has in a rewards program are shared with the consumer, and are necessary in order for the consumer to be able to use those rewards. Because these data are shared with consumers, must be shared for rewards programs and products to function, and are necessary for consumers to comparison shop and make informed choices about how to use their account, they are not confidential commercial information.

With respect to a commenter that suggested the CFPB should further define confidential commercial information on the basis of data's utility to a consumer relative to its commercial value to a data provider, the CFPB has determined that this suggested additional restriction of data availability is inconsistent with Congress's delineation of limited exceptions to the consumer access data right. Congress did not include an additional balancing test in CFPA section 1033, and imposing one in this final rule would risk subverting consumers' right to access data. However, the CFPB notes that the § 1033.421(a) general limitation standard limits third parties' collection, use, and retention of covered data to that which is reasonably necessary to provide the product or service that the consumer requested. If particular data points are not relevant to any product or service that a consumer might request, then a third party would generally not be able to request those data points. In this way, the final rule already accommodates the commercial usefulness of covered data without the inclusion of an explicit balancing test.

With respect to information that cannot be shared for contractual reasons and attorney work product related to an account and any active litigation, commenters did not identify specific

items of covered data that would potentially fall under these conditions. A data provider cannot limit a consumer's access to data simply because the consumer and the data provider are engaged in a legal dispute. While there is a separate exception for data that must be kept confidential by any other provision of law, as discussed later in this section this exception does not apply merely because the data provider must protect it for the consumer. Furthermore, if a data provider were to structure legal arrangements with the intent of subjecting covered data to this exclusion with the likely effect of frustrating consumers' data access rights, such behavior could violate the anti-evasion provision in final § 1033.201(a)(2).

For a discussion of comments related to reverse engineering of covered data, see part IV.D.3.

Information collected for the sole purpose of preventing fraud and certain other unlawful activities

Final § 1033.221(b) restates the exception at section 1033(b)(2) any for information collected by the 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. Final § 1033.221(b) further clarifies that information collected for other purposes does not fall within this exception, and states that, for example, name and other basic account verification information do not fall within this exception. The final rule retains the word "sole" because the CFPB understands that data providers use a variety of data in the context of identifying and preventing unlawful activity, and therefore expanding the exception to cover all information used for these purposes would create an exception that risks swallowing the rule.

Similarly, basic account verification information is necessary to support a variety of use cases for which the third party needs to ensure that the name on the account matches the name of

the consumer. Expanding the exception to cover this kind of basic data—which is collected by data providers for a variety of reasons unrelated to preventing unlawful activity—would frustrate consumers' data access right in a way that would conflict with Congress's intent.

Information required to be kept confidential

Final § 1033.221(c) restates the exception at section 1033(b)(3) for any information required to be kept confidential by any other provision of law. Final § 1033.221(c) further clarifies that information does not qualify for this exception merely because the data provider must protect it for the consumer. Final § 1033.221(c) also states, as an example, that the data provider cannot restrict access to the consumer's own information merely because that information is subject to privacy protections. In response to comments requesting that the CFPB identify laws that might require information to be kept confidential, the final rule does not include specific examples, because of the potential for both over- and under-inclusiveness. However, the CFPB notes that, as an example, financial institutions are prohibited from notifying an individual that a suspicious activity report has been filed against them, and this might constitute an example of when a data provider would be required to keep that specific information confidential.

In response to comments requesting a good faith compliance standard for data providers to withhold information if they reasonably believe that the information must be kept confidential by law, the CFPB notes that, under final § 1033.351(b)(1), indicia of whether a data provider's record of data fields it makes available complies with the policies and procedures requirement of final § 1033.351(b) include whether that record conforms to a consensus standard. Thus, to the extent that a data provider conforms with a consensus standard in making particular data fields

available (and not making other data fields available), conformance with the consensus standard would carry some indication of compliance.

Information that cannot be retrieved in the ordinary course of business

Final § 1033.221(d) restates the exception at CFPA section 1033(b)(4) for any information that the data provider cannot retrieve in the ordinary course of its business with respect to that information.

Terms and conditions information is typically retrievable in the ordinary course of business as data providers are required to disclose and make available such information under other laws, including but not limited to Regulation E and Regulation Z.[59] The other suggestions raised by commenters—such as security incident information and one-time verification codes—generally do not fall within the covered data definition in § 1033.221 or otherwise are not in the control or possession of the data provider. For example, as discussed above in part IV.B.3 with respect to upcoming bill information, bill payments scheduled directly with merchants or other payees—and not on the data provider's bill payment platform—are not typically in the control or possession of the data provider. Generally, a data provider would not be permitted to categorically refuse access to data specifically included in the definition of covered data under this exception, absent some additional showing that the data were not retrievable in the ordinary course of its business with respect to that information. The CFPB understands from comments that historical terms and conditions information may sometimes be stored as image files. If it would require extraordinary, manual effort to collect and translate this information into a

[59] For example, 12 U.S.C. 4303(a) of the Truth in Savings Act (TISA), 12 U.S.C. 4301 *et seq.* states: "Each depository institution shall maintain a schedule of fees, charges, interest rates, and terms and conditions applicable to each class of accounts offered by the depository institution, in accordance with the requirements of this section and regulations which the [CFPB] shall prescribe." Further, 12 U.S.C. 4305(a) requires a depository institution to make the required schedule available to any person upon request. TISA is implemented in the CFPB's Regulation DD (12 CFR part 1030) and the NCUA's 12 CFR part 707.

machine-readable, electronic form, that information may not be retrievable in a data provider's ordinary course of business with respect to that information. However, the CFPB does not expect current terms and conditions to be subject to any such exception given the legal requirements noted above.

One commenter asked the CFPB to lower the historical transaction data safe harbor in § 1033.211(a) from 24 months to 6 months because it does not believe that 24 months of transaction data are retrievable in the ordinary course of business. As discussed above in § 1033.211(a), the CFPB understands that data providers generally retain 24 months of transaction data according to their record retention requirements in Regulation E and Regulation Z. If a data provider cannot retrieve 24 months of data in the ordinary course of business notwithstanding its other compliance obligations, it cannot take advantage of the safe harbor but would be able to make available less information. With regard to comments requesting that this section include a prohibition on reverse engineering, such a prohibition would not be appropriate for exceptions to the requirement to make available covered data. However, third party use of data for reverse engineering of proprietary algorithms is addressed in the discussion of § 1033.421(a)(2).

In response to the comments suggesting that the final rule narrow this exception to avoid evasion of the final rule, this concern is addressed in the anti-evasion provision in final § 1033.201(a)(2). A data provider that designs its systems to make data less available to access, with the intent of evading the requirements of subparts B and C of part 1033, or that the data provider knows or should know is likely to render unusable covered data or is likely to prevent, interfere with, or materially discourage a consumer or authorized third party from accessing covered data, would violate the anti-evasion provision.

C. Subpart C—Data Provider Interfaces; Responding to Requests

1. Overview

Subpart C establishes how covered data are to be made available and the mechanics of data access, including basic operational, performance, and security standards, and other policies and procedures. In particular, certain provisions ensure that data providers make covered data available to authorized third parties through functionality fit for that purpose—labeled a "developer interface"—rather than through screen scraping of a consumer interface. Other provisions require data providers to disclose information that helps third parties request data and to establish and maintain written policies and procedures reasonably designed to achieve the objectives of subparts B and C. In addition, to prevent data providers from inhibiting consumers' exercise of their statutory data access right, subpart C prohibits data providers from charging fees for establishing or maintaining the required interfaces or for receiving requests or making available covered data in response to requests.

2. General requirements (§ 1033.301)

Requirement to maintain interfaces (§ 1033.301(a))

The CFPB proposed in § 1033.301(a) to require a data provider subject to the requirements of part 1033 to maintain a consumer interface and to establish and maintain a developer interface. The CFPB preliminarily determined that the requirement would carry out the objectives of CFPA section 1033 by ensuring consumers and authorized third parties can make requests for and receive timely and reliable access to covered data in a usable electronic form. Proposed § 1033.301(a) also stated that the consumer interface and the developer interface must satisfy the requirements set forth in § 1033.301 (*i.e.*, § 1033.301(b) and (c), discussed in

this part IV.C.2 below) and that the developer interface must satisfy the additional requirements set forth in § 1033.311 (discussed in part IV.C.3 below).

Requirement to maintain consumer interface

Under the CFPB's proposal, not every interface that a data provider might offer—such as a mobile banking portal and an online banking portal—would have been required to satisfy all of the proposed requirements that would apply to consumer interfaces (discussed below), as long as collectively the provider's interfaces satisfy the requirements. The CFPB requested comment on whether data providers inform consumers using mobile banking applications that additional information might be available through providers' online banking applications.

All commenters, including data providers, third parties, and consumer advocate commenters, who addressed the requirement to maintain a consumer interface supported it. Data providers stated that they maintain those interfaces today. Consumer advocates suggested that the CFPB adopt additional requirements for consumer interfaces, such as being intuitive or user friendly. They also suggested that the rule require a data provider to disclose in the consumer interface the third parties accessing a consumer's covered data and, if the data provider provides a mechanism for the consumer to revoke such access, how the consumer can revoke such access. They argued that these disclosures are important to facilitate consumer awareness of the third parties with which they have shared their data and consumer action if they do not want the data sharing to continue. In response to the CFPB's request for comment, they requested that the CFPB require a data provider to provide through its mobile application the same information as through a desktop application, because many low- and moderate-income consumers only have a mobile phone for Internet access.

For the reasons discussed herein, final § 1033.301(a) requires a data provider to maintain a consumer interface. This is necessary and appropriate to implement the statutory requirement in CFPA section 1033(a) that data providers make covered data available to consumers in a usable electronic form. The requirement will impose limited cost on data providers because they generally maintain these interfaces today. It will ensure that consumers benefit from ready access to their own financial data.

The CFPB declines to adopt the additional requirements for the interfaces suggested by consumer advocates. Under the final rule, as under the proposal, not every data provider consumer interface must satisfy the requirements of part 1033, as long as collectively the provider's consumer interfaces satisfy the requirements. Competition among data providers for customers will continue to appropriately incentivize them to invest in and improve the various consumer interfaces they make available to consumers. In contrast, the CFPB is adopting more prescriptive requirements for developer interfaces in § 1033.311 (discussed below) because consumers are unlikely to comparison shop among data providers based on the performance of those interfaces.

Requirement to maintain developer interface

The CFPB received numerous comments related to its proposal in § 1033.301(a) to require data providers to establish and maintain a developer interface. Third party commenters requested clarification as to how the provision would apply to a service provider that the data provider employs to establish and maintain the data provider's developer interface. More specifically, they requested that the rule clarify that, in such a situation, the data provider's service provider may not impose any conditions or restrictions on interface access that the data provider itself may not impose and must comply with all rule provisions applicable to developer

interfaces. Commenters of all types—including third parties, consumer advocates, research and academic institutions, data providers and associations thereof—expressed general support for the CFPB's framework in part 1033 of moving away from screen scraping for data access, but requested technological neutrality for how a data provider may implement the required interface. Some commenters, including both data providers and third parties, stated that implementing APIs would be overly difficult or costly for some data providers such as small depository institutions. These commenters requested that the rule allow data providers the choice of implementing a developer interface, permitting screen scraping of the consumer interface, or prohibiting access to covered data by all third parties.

Some data provider commenters and a data aggregator questioned or objected to the CFPB's proposal to require data providers to establish a developer interface. These commenters asserted that the requirement is beyond the authority CFPA section 1033 provides to the CFPB and that it is in their view not appropriate for a regulation, as opposed to a statute, to require entities to implement what they characterized as a new financial product such as a developer interface. In particular, these commenters asserted that the CFPB had incorrectly interpreted the term "consumer" to include consumers' third party representatives. They also asserted that the CFPB lacked authority to require data providers to enable "open banking," which they described as a matter of vast economic and political significance subject to the "major questions" doctrine.

One commenter stated that Congress could not have intended this broad result because in 2010, when Congress adopted the CFPA, the data sharing market did not include the wide variety of third party fintech firms that the CFPB proposed to include as consumers. The commenter also stated that the proposal was inconsistent with the structure of CFPA section 1033 because it would require a developer interface that is exclusively accessible to third parties

and a consumer interface that is exclusively accessible by consumers. The commenter also maintained that Congress would not have intended section 1033 to authorize the CFPB to launch open banking unilaterally without providing for a greater role for other agencies, beyond what it described as a narrow degree of consultation about certain topics. The commenter did not believe the CFPB had given those agencies a meaningful role in the process. Finally, the commenter stated that efforts to create an open banking system would restrict technological innovation and consolidate the number of incumbent data aggregators in the market.

For the reasons discussed herein, the CFPB is finalizing the requirement in § 1033.301(a) that a data provider maintain a developer interface. No change in substance from the proposal is intended or effected by simplifying the proposed rule's "establish and maintain" to "maintain" in final § 1033.301(a). Under the proposed rule, a data provider was exempt from the proposal if it did not have a consumer interface. The CFPB proposed that a data provider with a consumer interface but without a developer interface would be required to "maintain" the consumer interface and to "establish and maintain" a developer interface. Under final part 1033, the question of whether a data provider has a consumer interface is not relevant to determining whether the data provider is subject to part 1033. A data provider subject to part 1033 must have functionality for making covered data available to consumers (a consumer interface) and functionality for making covered data available to authorized third parties (a developer interface). If a data provider subject to part 1033 does not currently have such functionality for authorized third parties, the part 1033 requirement that the data provider maintain such functionality—a "developer interface"—includes and incorporates the proposed requirement that the provider establish the developer interface.

The requirement is necessary and appropriate to ensure data providers make available covered data upon request in a usable electronic form to third parties that are authorized to access covered data on behalf of consumers. The developer interface requirements in the rule, including the requirement that the interface not allow third parties to access covered data using consumer credentials, are not a requirement to use any specific technology to enable data access. As discussed under the definitions above, the term "developer interface" is simply a label of convenience for data access functionality that meets rule requirements. The technological means by which data providers choose to achieve that functionality is entirely up to providers.

The requirements and prohibitions in subparts B and C of part 1033 apply to data providers. A data provider may not by contract transfer its legal obligation to comply with the part 1033 requirements and prohibitions to a vendor. A data provider may enter into a contract with a vendor under the terms of which the vendor agrees to perform activities that satisfy the data provider's compliance obligations under part 1033, but in that situation it remains the data provider's legal responsibility to comply with the requirements and prohibitions of subparts B and C of part 1033, and the data provider violates part 1033 if its vendor fails to fully fulfill the relevant compliance obligations. For example, if the data provider and its vendor collectively fail to fully fulfill one or more of the data provider's obligations under part 1033, the CFPB (or other regulator) may supervise and enforce that compliance failure against the data provider.

In final part 1033, the CFPB has taken steps to ensure the feasibility and technological neutrality of the § 1033.301(a) requirement that a data provider maintain a developer interface, including for small data providers. The final rule does not require the use of any specific technology in order to comply. Specifically, in § 1033.311(e) (discussed in part IV.C.3 below), the CFPB is incorporating an example that makes explicit that a data provider may satisfy its

obligation to maintain the required data access by entering into a contract with its service provider (for example, a core processor) pursuant to which the service provider screen scrapes covered data from the data provider's consumer interface and makes the covered data available to authorized third parties through a developer interface that the service provider maintains on behalf of the data provider. The CFPB believes that this "self-scraping" approach will meaningfully reduce the burden of the developer interface requirement through economies of scale: a small number of larger service providers will be able to maintain developer interfaces on behalf of a large number of smaller data providers. In this situation, as discussed above, the obligation for the developer interface to satisfy the requirements and prohibitions of part 1033 nonetheless continues to rest with the data provider.

The CFPB has determined that the CFPA provides the CFPB with authority to require data providers to maintain developer interfaces and that the rule does not run afoul of the major questions doctrine. As proposed (and as discussed above), § 1033.131 defines "developer interface" as functionality through which a data provider receives requests for covered data from authorized third parties and makes covered data available electronically in response to the requests. Requiring data providers to maintain this functionality does not constitute requiring them to provide a new consumer financial product or service; instead, it merely requires them to maintain a secure mechanism through which they make consumers' covered data available to consumers' authorized third party representatives. Elsewhere in this notice, the CFPB estimates the costs part 1033 will impose on data providers (including but not limited to the developer interface requirement). The costs are orders of magnitude lower than any level that would implicate the major questions doctrine. There is also no political controversy on the topic of developer interfaces of the magnitude that suggests it is a major question.

To the extent that commenters meant to argue that requiring data providers to provide covered data to consumers' authorized third party representatives implicates the major questions doctrine, the CFPB disagrees. As noted above, the costs of providing covered data to third parties are orders of magnitude lower than any level that would implicate the major questions doctrine, and there is also no political controversy of the kind that has supported a finding that there is a major question. Moreover, the plain meaning of CFPA section 1033, in combination with the CFPA's definition of consumer in CFPA section 1002(4), requires data providers to make covered data available to consumers' authorized third party representatives. Thus, any purportedly "major" consequences from that requirement flow from Congress' decision to enact 1033, not the CFPB's rule. This is not a situation where an agency discovers in a long-extant statute an unheralded power. Instead, this is simply the first CFPB rule to execute Congress' instructions on the topic, after a multiyear rulemaking process.

The CFPB notes that the U.S. consumer data sharing market encompassed consumers' authorized third party representatives at the time Congress enacted the CFPA in 2010. For example, many consumer-authorized third party representatives were providing personal financial management use cases well before 2010.[60] Thus, Congress in fact did intend that the 2010 CFPA and the CFPB's rule implementing it (as expressly authorized by CFPA section 1033(a)) would broaden and deepen the consumer-permissioned data sharing market that existed at that time by requiring data providers to share financial data with consumers' authorized third

[60] Pre-2010 providers of these use cases include Mint, Mvelopes, Quicken, Wesabe, and Yodlee.

party representatives. And nothing in the language of CFPA section 1033 limits it to the use cases that existed in 2010.[61]

This view of congressional intent is fully consistent with the plain meaning of CFPA sections 1033 and 1002(4) described above, the interoperability objectives of CFPA section 1033(d), and the ongoing evolution of the U.S. data sharing market. That is, a rule requiring only that data providers make financial information available to individual consumers, as opposed to also requiring them to make the information available to third parties authorized by consumers, would significantly impair the uses to which consumers, through authorized third parties, are actually putting their financial data today. In sum, therefore, the CFPB can discern no textual, historical, or consumer-protection basis for limiting part 1033 in the artificially cramped way that these commenters suggest.

Similarly, "open banking" as the CFPB uses that term (which is not legally defined) already exists in the U.S. The proposed rule noted that the CFPB "uses the term 'open banking' to refer to the network of entities sharing personal financial data with consumer authorization." 88 FR 74796, 74797 (Oct. 31, 2023). U.S. data providers already do that. Further, such sharing is what CFPA section 1033 mandates and what part 1033 requires. Of course, other jurisdictions might use the term "open banking" differently. For example, part 1033 does not require data providers to permit authorized third parties to *make changes* (commonly referred to as "write access") to consumers' financial data or to transfer funds to or from consumers' financial accounts. In contrast, other "open banking" frameworks around the world, such as the European Union Payment Services Directive and the United Kingdom's Open Banking framework, address

[61] To the contrary, Congress intended for the CFPB to have "enough flexibility to address future problems as they arise," and that "[e]xperience has shown that consumer protections must adapt to new practices and new industries." S. Rep. 111-176 at 11 (2010).

write access. While these limitations might be in contrast to other jurisdictions' use of the term "open banking," such semantics do not change the fact that part 1033 adheres closely and appropriately to the open-banking framework Congress enacted in CFPA section 1033.

The CFPB also finds that the part 1033 developer interface requirement is justified by the factual record and will not stifle innovation nor result in anti-consumer consolidation. Specifically, the rulemaking record provides ample evidence that a CFPB regulation condoning or requiring data provider provision of consumers' data to authorized third parties through the mechanism of screen scraping of data providers' consumer interfaces would present inappropriate data security and data accuracy risks to consumers, as well as to data providers, and would reduce consumers' control over the portion of their financial data that they share. The CFPB finds that the permitted self-scraping approach described above does not entail these risks because data providers contractually govern and are responsible for the "self scraping" that data providers' service providers, such as core processors, will conduct under that approach.

The CFPB considered a form of screen scraping known as "tokenized" screen scraping, which is more secure than regular screen scraping. However, even tokenized scraping results in third parties accessing a larger portion of consumers' financial data than they need to provide the financial services that consumers are requesting. Like non-tokenized screen scraping, it also requires third parties to parse and transpose financial information from human-readable form. The CFPB received feedback that this activity risks inaccuracy and undermines the interoperability benefit of standardized data formats, which CFPA section 1033(d) requires the CFPB to promote. Such data would not be usable to consumers or authorized third parties, as required by CFPA section 1033(a). The CFPB therefore is not adopting that alternative.

In light of the risks and imprecision of screen-scraping , and within the bounds of the rulemaking discretion granted to it by CFPA section 1033(a), the CFPB has determined that the best way to effectuate the CFPA requirement that data providers make covered data electronically available to consumers' authorized third party representatives, and also make the data available securely and accurately, is to require data providers to maintain a "developer interface," *i.e.*, to maintain functionality fit for purpose through which they electronically receive and respond to requests for covered data from authorized third parties in accordance with the requirements of part 1033. As noted, CFPA section 1033(a), in combination with the CFPA's consumer definition, makes clear that the CFPA requires data providers to make covered data available to consumers' authorized third party representatives. The CFPB therefore declines to permit a data provider to comply with CFPA section 1033(a) by blocking all third party access to covered data.

Some commenters asserted that this approach would restrict technological innovation or result in consolidation of the data aggregation market. As noted above, the rule implements Congress' decision for data providers to make available consumer data to third parties directly. Further, the rule will foster competition and innovation, as many commenters believed it would. In particular, the standardization and machine-readability of data types and formats and communications protocols across data providers that is enabled by developer interface functionality, as opposed to screen scraping, will facilitate, not restrict, direct access to consumers' financial data by authorized third parties, including new entrants and those providing products and services that compete with those offered by the consumer's existing account provider. That is, it will reduce authorized third parties' reliance on data aggregators for accessing consumers' financial data from data providers. This is because screen scraping—the

data ingestion, parsing, and mapping it entails (let alone all its risks and inaccuracies)—is not easy, which is why many smaller authorized third parties today rely on data aggregators to do it. Because the standardization enabled by developer interfaces will facilitate direct access by authorized third parties, the number of authorized third parties should increase (the opposite of consolidation) and the variety of products and services they offer should also increase (the opposite of restricting innovation). Further, competition among data aggregators for the business of authorized third parties should increase too.

It is also not true, in contrast to commenters' assertions, that part 1033 requires a data provider to maintain developer interface functionality that is *exclusively* accessible by authorized third parties and a consumer interface that is exclusively accessible by individual consumers. Instead, part 1033 permits (but does not require) data providers to grant developer interface access to individual consumers and to grant consumer interface access to authorized third parties. Further, part 1033 does not require that a data provider's consumer interface and its developer interface be separate and distinct from each other. Instead, part 1033 permits (but does not require) a data provider to provide its developer interface and its consumer interface through the same mechanism (or set of mechanisms), provided that the mechanism satisfies the part 1033 requirements applicable to developer interfaces and the requirements applicable to consumer interfaces.

The CFPB discusses elsewhere in this final rule the consultation processes that it has engaged in with Federal and State regulators. In contrast to commenters' assertions, the CFPB in fact gave other agencies a very meaningful role in the process and, in any event, has complied with the consultation obligations that the law places on the CFPB.

Machine-readable files (§ 1033.301(b))

The CFPB proposed in § 1033.301(b) to require a data provider to make available, upon specific request, covered data in a machine-readable file that can be retained by a consumer or an authorized third party and transferred for processing into a separate information system that is reasonably available to and in the control of the consumer or authorized third party. The CFPB also proposed an example of how data providers could make available covered data in a machine-readable file that can be retained. The CFPB preliminarily determined that § 1033.301(b) would provide important benefits to consumers, such as by enabling them to share their data with others, including providers of competing financial products and services.[62]

Consumer advocate and third party commenters generally did not address the proposed § 1033.301(b) requirement.[63] Data provider commenters did not object to it, but suggested modifications and clarifications. They requested that the provision differentiate more clearly between developer and consumer interfaces, arguing that their file formats are, and should remain, different from each other. They also requested that the rule define "machine-readable," particularly with respect to the consumer interface. They noted that the proposed rule preamble stated the CFPB's view that today's consumer interfaces generally perform in an acceptable manner and that the CFPB did not intend its proposal to result in material changes to consumer interfaces. Some commenters asserted, however, that the proposed provision could be interpreted to include burdensome requirements for the consumer interface. They stated that data providers' consumer interfaces today typically make covered data available in PDF files that consumers can

[62] *See, e.g.*, Michael S. Barr *et al.*, *Consumer Autonomy and Pathways to Portability in Banking and Financial Services*, Univ. of Mich. Ctr. on Fin., L. & Policy Working Paper No. 1 (Nov. 1, 2019), https://financelawpolicy.umich.edu/sites/cflp/files/2021-07/umich-cflp-working-paper-consumer-autonomy-and-data-portability-pathways-Nov-3.pdf.

[63] One third party stated that machine-readable formats would advance self-sovereign-identity principles.

print and download, but do not make all covered data available in a single file, nor do they make all covered data available in files that are machine-readable (such as CSV, XLS, or XML files) but instead only make transaction history available in such files. They asserted that if proposed § 1033.301(b) were interpreted to include such requirements—*e.g.*, that all of a consumer's covered data be made available in a single machine-readable file through the consumer interface—the provision would result in costly modifications to data providers' consumer interfaces when only few consumers actually request machine-readable files through consumer interfaces. One commenter expressed fraud concerns with respect to making machine-readable files available through the consumer interface but did not elaborate.

The CFPB is finalizing § 1033.301(b) with certain changes. Except as discussed below, the provision requires that upon request for covered data in a machine-readable file, a data provider must make available to a consumer or an authorized third party covered data in a file that is machine-readable and that the consumer or authorized third party can retain and transfer for processing into a separate information system that is reasonably available to and in the control of the consumer or authorized third party. These requirements will provide important benefits to consumers, such as by ensuring that they continue to be able to share their data with others, including providers of competing financial products and services. However, to ensure these benefits without imposing inappropriate burden on data providers, particularly with respect to their consumer interfaces, it is necessary and appropriate to differentiate between the consumer interface and the developer interface, to not apply certain requirements to the consumer interface, and to provide clarity regarding how the developer interface satisfies the requirements, as follows.

Data providers' consumer interfaces generally provide covered data to consumers in an acceptable manner. The CFPB intends and expects that its final rule will not require material changes to data providers' existing consumer interfaces. Unlike the proposal, the final rule for consumer interfaces, as set forth in § 1033.301(b)(1)(i), does not apply the machine-readability requirements of § 1033.301(b) to payment initiation information (described in § 1033.211(c)) or to account verification information (described in § 1033.211(f)). Nonetheless, the consumer interface is required to make that information available in an electronic form usable by consumers, such as a human-readable form, pursuant to the general availability requirement in § 1033.201(a). In contrast to how this information must be made available to third parties through the developer interface, requiring this information be made available directly to consumers in machine-readable files would provide limited additional utility to consumers relative to their ability to access this information in human-readable form.

Moreover, and also unlike the proposal, pursuant to § 1033.301(b)(1)(ii), the final rule does not require consumer interfaces to make available the account terms and conditions (described in § 1033.211(d)) in machine-readable form. Instead, that information need only be made available in a retainable form. Many data providers make terms and conditions available to consumers, as well as the general public, in retainable form. The CFPB understands that data providers generally also make certain important terms and conditions—such as the rates and fees applicable to accounts and balances—available in human-readable form in the consumer interface; additionally, many terms and conditions applicable to accounts are restated in periodic statement communications, which are also generally made available through consumer interfaces. The CFPB intends and expects that these changes from its proposed rule will mean that the requirements of § 1033.301(b) for consumer interfaces do not result in material burden

for data providers; *i.e.*, do not result in material changes from data providers' current consumer interface systems and practices.

For consumer interfaces, the covered data that remains subject to § 1033.301(b) is the following: transaction information (described in § 1033.211(a)), account balances (described in § 1033.211(b)), and upcoming bill information (described in § 1033.211(e)). Data providers' consumer interfaces today generally make that portion of covered data available to consumers in machine-readable files. Accordingly, applying the requirements of § 1033.301(b) to that portion of covered data will not require material changes to data providers' existing consumer interfaces.

In final § 1033.301(b), the CFPB has deleted the word "specific" (*i.e.*, has deleted it from the proposal's phrase "upon specific request"). The CFPB neither intends nor effectuates any change of substance by this revision. It remains the case, as under the proposal, that the consumer must explicitly request covered data in a machine-readable file in order for the requirements of § 1033.301(b) to be triggered. While the rule does not specify the functionality (or functionalities) that a data provider must supply to consumers through which they may request covered data in machine-readable form, the data provider must supply at least one readily discoverable mechanism through which consumers may do so. It is acceptable for a data provider to supply the mechanism only to consumers who have "logged in." It is also acceptable for the data provider to guide consumers to the mechanism. For example, if a consumer calls the data provider, the provider may verbally guide the consumer to the mechanism. Similarly, if a consumer emails the data provider, the provider may reply by email with a link to or instructions for how to access the mechanism. Further, the data provider's mechanism should not require a consumer to say "magic words" in order for the data provider to deem the consumer to have requested data in machine-readable form. For example, if a consumer were to request "a

spreadsheet" of transactions, the data provider should consider the consumer to have requested a machine-readable file.

Like the proposal, final § 1033.301(b) does not require a data provider to make all covered data available to a consumer in a single file—for example, the entirety of the consumer's transaction history with the data provider in one file. It does (like the proposal) require the provider to make the data available to the consumer in one or more files. Section 1033.211(a) provides that a data provider is deemed to make available sufficient historical transaction information if it makes available at least 24 months of such information. It is feasible for the provider to make available that amount of historical information in one file. The provider could also make the information available in multiple files if it chooses to do so.

The requirement to make portions of covered data available in machine-readable files through the consumer interface, as described above, will not result in inappropriate fraud risk. As noted, the requirement is consistent with data providers' existing practices for making data available through their consumer interfaces. Further, the requirements in part 1033 to make covered data available (whether in machine-readable files or otherwise) do not include any requirement to permit consumers or authorized third parties to initiate payments through the consumer interface. Instead, it remains up to a data provider's discretion—as opposed to a requirement of part 1033 or any other CFPB rule—whether to grant consumers permission to initiate payments through the data provider's consumer interface.

With respect to the requirement in proposed § 1033.301(b) that a data provider make covered data available through its *developer* interface in machine-readable form, the CFPB has determined that the requirement in § 1033.311(b) (discussed below) that the developer interface make the covered data available in a standardized and machine-readable format is sufficient.

Section 1033.301(a) requires a data provider to maintain a developer interface, which § 1033.131 defines as 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. Further, § 1033.311(b)(2) requires the developer interface to make available covered data in a standardized and machine-readable format. A data provider that maintains a developer interface, as required by § 1033.301(a) and defined by § 1033.131, that complies with § 1033.311(b) thereby makes available to authorized third parties covered data in a machine-readable form that the authorized third parties can retain and process in separate information systems reasonably available to them. Accordingly, § 1033.301(b)(2) states that a data provider's developer interface satisfies the requirements of § 1033.301(b) if the interface makes available covered data in a form that satisfies the requirements of § 1033.311(b).

Fees prohibited (§ 1033.301(c))

The CFPB proposed in § 1033.301(c) to prohibit a data provider from imposing any fees or charges on a consumer or authorized third party for establishing or maintaining the interfaces required by § 1033.301(a) or for receiving requests or making available covered data in response to requests as required by part 1033. The CFPB preliminarily determined that the proposed prohibition was necessary and appropriate to ensure that fees do not impede consumers and authorized third parties from exercising consumers' statutory rights. The CFPB requested comment on whether any clear parameters exist such that, subject to such parameters, data providers could charge reasonable, standardized fees that neither obstruct the access right due to cost nor impede third parties' access to data provider interfaces due to negotiations over fee amounts or schedules.

Few commenters addressed the prohibition of fees for providing covered data to individual consumers through the consumer interface. Those commenters who addressed this issue did not object and stated that data providers do not charge fees today for providing covered data through their consumer interfaces.

Many commenters addressed fees for providing covered data to authorized third parties through the developer interface. Third party and consumer advocate commenters generally supported the proposed fee prohibition on the grounds that covered data belongs to consumers and that the statute gives consumers the right to access and share the data with the authorized third parties that they choose. These commenters also suggested modifications to the prohibition to ensure that data providers do not evade it by, for example, charging higher fees for other financial products and services to consumers and authorized third parties for exercising their section 1033 data access rights. Third party commenters suggested that the CFPB make clear that the fee prohibition applies to data providers' service providers, in addition to applying to data providers themselves.

SBA Advocacy compared data providers' provision of covered data to Federal agencies' provision of information in response to Freedom of Information Act (FOIA), 5 U.S.C. 552, requests and stated that it seems inconsistent that agencies are permitted to charge for providing information whereas data providers are prohibited from doing so.

Data provider commenters opposed the developer interface fee prohibition. They asserted that the CFPB lacks authority to prohibit fees under CFPA section 1033. They also stated (as noted above) that they would incur costs to implement the developer interface and that, in light of those costs, the fee prohibition is an impermissible taking because it commandeers data providers' infrastructure and resources for the benefit of third parties, which may access covered

data without paying a fee and then charge fees to other third parties for the data. These commenters also stated that the prohibition is inconsistent with the CFPB's 1034(c) advisory opinion, which permits large institutions to charge fees for providing data in some limited circumstances, such as where a consumer had already repeatedly requested and received the same information regarding their account. It is also inconsistent, they stated, with OCC regulations (12 CFR 7.4002), which according to the commenters give national banks discretion to set prices for the banking services they provide. No commenters provided any information regarding possible parameters for standardized fees.

For the reasons discussed herein, consistent with the proposal, final § 1033.301(c) prohibits a data provider from imposing any fees or charges on a consumer or authorized third party for establishing or maintaining the interfaces required by part 1033 or for receiving requests or making covered data in response to requests as required by part 1033. This prohibition ensures that data providers do not inhibit consumers' ability to access their data, authorize third parties to access their data, or choose which third parties to authorize to access their data.

The CFPB is issuing § 1033.301(c) pursuant to its authorities under sections 1033(a) and 1022(b)(1) of the CFPA. Section 1033(a) states that data providers "shall" make covered data available to consumers "upon request," "[s]ubject to rules prescribed by the Bureau," subject to certain statutory exemptions in section 1033(b), and without any other condition. Congress did not authorize fees. In fact, it specified in section 1033(b)(4) that a data provider need not make available information it "cannot retrieve in the ordinary course of its business," which weighs against an argument that Congress intended data providers to be able to decide to condition data access on payment of a fee. Congress dealt with the policy issue of potential burden on data

providers by cabining the information they are required to retrieve, rather than through compensation. Even assuming Congress did not foreclose fees when consumers exercise their statutory rights under section 1033, in exercising the CFFB's rulemaking authority to regulate the specifics of data sharing under section 1033, the CFPB is not permitting fees. In particular, the CFPB is concerned that allowing them would obstruct the data access right that Congress contemplated. As discussed later, the CFPB has not identified, and no commenter has put forward, a suitable alternative that protects the data access right.

The fee prohibition is also independently authorized by section 1022(b)(1) of the CFPA in order to prevent evasion of Federal consumer financial law. CFPA section 1033 and this final rule are both Federal consumer financial laws. If data providers could decide what fee to charge, they could limit or eliminate the right that CFPA section 1033 confers. Congress would not have enacted CFPA section 1033 if it trusted data providers to be fully forthcoming with covered data. And, in the CFPB's assessment, those data providers that perceive CFPA section 1033 to be a threat to their competitive positions have strong incentives to withhold information. The CFPB has not identified a suitable alternative that would prevent such evasion of the data access right.

The CFPB notes that the fee prohibition is far from a novel use of rulemaking authority. Other longstanding consumer financial regulations prohibit fees when consumers seek to exercise statutory rights under Federal consumer financial laws that are otherwise silent on whether an entity may charge fees. For example, Regulation E (12 CFR part 1005) and Regulation Z (12 CFR part 1026) both prohibit fees for error resolution when an error has occurred and require avoidance of "any chilling effect on the good-faith assertion of errors that might result if charges are assessed when no billing error has occurred."[64]

[64] Regulation E comment 11(c)-3; Regulation Z comment 13-2.

The CFPB also notes that the fee prohibition is not inconsistent with FOIA. There, the applicable statute expressly permits fees, whereas here it does not. Further, the information agencies provide through FOIA typically does not pertain directly to the requestors of the information, whereas under CFPA section 1033 the information provided by data providers pertains directly to the requestor—the consumer—because it is information about the financial product or service the consumer obtained from the data provider. Finally, FOIA addresses information that may not be readily available for agencies to find and disclose, whereas CFPA section 1033 addresses information that data providers can retrieve in the ordinary course of business.

The fee prohibition does not make this rule a taking. The addition of the fee prohibition does not make the rule a permanent physical invasion of property, nor does it limit data providers' control or discretion to the point that they are deprived of all economically beneficial use of property. Further, data providers do not generally charge consumers or third parties for data access today, indicating that the economic impact of the prohibition, along with any potential interference with investment-backed expectations, is not so large as to be considered a taking. Any hypothetical investment-backed expectations are further attenuated by the fact that Congress enacted section 1033 over fourteen years ago, and the CFPB has been engaged in a lengthy rulemaking process which will be followed by staggered compliance dates over a period of years. Data providers have long been on notice that a CFPB rulemaking will impact data sharing. The character of this rule is also far removed from a taking. The rule adjusts the benefits and burdens of economic life, specifically by providing consumers with greater access to data about their financial accounts, in some cases with the assistance of companies acting as their representatives.

The fee prohibition is not inconsistent with CFPA section 1034(c) which, as noted in the CFPB's advisory opinion, permits fees in certain limited circumstances, such as when a large bank or credit union charges a fee to a consumer who repeatedly requested and received the same information regarding their account. *See* 88 FR 71279, 71282 (Oct. 16, 2023). Section 1034(c) imposes an obligation to "comply" with a consumer request for information, and the CFPB explained that, in the context of repeated requests, the large bank or credit union would have already met its obligation under section 1034(c) by "comply[ing]" with the consumer's earlier requests. *Id.* By contrast, section 1033 imposes an obligation to "make available" information upon the consumer's request. 12 U.S.C. 5533(a). By referring to information being made "available," section 1033 contemplates an ongoing obligation to grant consumers access to information, rather than an obligation that could be satisfied by providing information a single time.

Moreover, the CFPB did not promulgate the CFPA section 1034(c) opinion through the notice-and-comment rulemaking process. As such, the opinion was and is limited to setting forth the CFPB's interpretation of existing law. In contrast, the CFPB is establishing part 1033 in accordance with the Administrative Procedure Act's notice-and-comment rulemaking procedures. The CFPB's promulgation of part 1033 may therefore establish new requirements, including by limiting fees more strictly than does section 1034(c), if the CFPB determines that is warranted using the discretionary rulemaking authority that Congress has delegated.

The fee prohibition is also not inconsistent with the OCC regulation cited by commenters. The OCC regulation, 12 CFR 7.4002, generally provides that national banks have authority to charge their customers non-interest charges and fees but does not override other Federal laws or regulations that expressly bar specific charges and fees. For example, as noted above, when an

error has occurred the CFPB's Regulation E and Regulation Z prohibit fees for resolving the error and the OCC's regulation does not override those prohibitions.

Data provider commenters additionally argued that part 1033 should permit them to charge fees because data providers' systems are key to making covered data available and establishing and maintaining those systems requires resources. They argued that a rule prohibiting them from offsetting those costs by charging fees to third parties could necessitate recoupment of the costs through fees to their consumer account holders for other banking services. They also argued that the fee prohibition would discourage data providers from implementing and investing in data sharing systems that exceed the minimum legal requirements. In contrast, they argued, permitting reasonable fees would incentivize both data provider investment and third party data minimization. That is, they argued, third parties accessing more data through developer interfaces would impose more burden on those interfaces and therefore should incur greater fees than those accessing less data. Data provider commenters also asserted that in other jurisdictions, such as the E.U., fee prohibitions have led to underinvestment and suboptimal open finance ecosystems. They further argued that in light of these considerations, E.U. rules proposed in November 2023 would permit data providers to request reasonable compensation when providing data to other businesses.

As part of the rulemaking process, the CFPB has taken steps to reduce data providers' data access costs, as reflected in the final rule. First, the CFPB proposed and is finalizing that data providers must make available a narrower set of covered data than the CFPB was considering at the SBREFA stage. Second, in contrast to the proposed rule, the final rule does not apply to depository institutions that are small businesses as defined in SBA's regulations (irrespective of whether those institutions have a consumer interface). These institutions

therefore will not incur any data access costs under the final rule. Third, many depository institutions that are not small businesses, and are therefore subject to part 1033, already have developer interfaces and therefore should be able to bring those interfaces into compliance with part 1033 at reasonable cost. Fourth, the final rule adopts a substantially more extended implementation timeframe than the CFPB proposed. Fifth, the CFPB continues to develop guidance materials and to work with industry standard setters to foster appropriate standards. These steps will give data providers more certainty regarding how to come into compliance with the rule in the extended implementation timeframe, thereby reducing their costs. And sixth, § 1033.311(e) (discussed in part IV.C.3 below) makes clear that a data provider's developer interface may function by permitting the data provider's service provider (such as a core processor) to screen scrape the data provider's consumer interface and to make the data available through a developer interface that the service provider establishes and maintains on the data provider's behalf. This approach offers data providers a low-cost path to providing a developer interface and is widely used in the market today.

The CFPB does not expect that the fee prohibition will discourage data providers from implementing and investing in their data sharing systems. The CFPB is not aware that regulatory requirements or prohibitions in other areas, such as Regulation E and Regulation Z error resolution, inappropriately discourage investment in systems in those areas. To the contrary, regulatory requirements and prohibitions encourage robust systems and make it less likely that an industry participant with such systems will be driven from the market by participants without them. Additionally, data providers generally invest significantly in continually improving their consumer interfaces, which data providers generally do not charge any kind of fees to access. The CFPB is also aware, including from the Provider Collection, that some data providers and

service providers (such as core providers) made significant investments to develop, implement, and maintain developer interfaces even prior to this rulemaking, and, as noted above, data providers do not generally charge fees to third parties for accessing developer interfaces.

Data provider fees are not the appropriate means by which third parties' data minimization is incentivized and accomplished. Instead, third parties themselves must and should comply with part 1033's data minimization requirements. Section 1033.311(d) (discussed below) permits data providers to impose reasonable access caps, further undermining the appropriateness of permitting data providers to charge fees to third parties in order to achieve data minimization or, more broadly, to incentivize third parties to comply with part 1033.

By its terms, the § 1033.301(c) fee prohibition applies to data providers and will be supervised and enforced against data providers (just like all of the other provisions in subparts B and C). But the fee prohibition encompasses a data provider's vendor, in addition to the data provider itself. For example, assume a data provider asserts that it is complying with part 1033 because it makes covered data available to authorized third parties through a developer interface that the data provider's vendor maintains on behalf of the data provider. The data provider would not comply with the fee prohibition in § 1033.301(c) if its vendor charged (or sought to charge) fees to authorized third parties in connection with making covered data available to them through the developer interface that the vendor maintains on behalf of the data provider.

Data sharing in the U.S. is distinguishable in relevant respects from the E.U. American consumers already expect third party data access capabilities, and the U.S. market consists of a higher number of depository institutions (and card issuers) than most other jurisdictions. Further, the E.U. proposal to permit fees is only a proposal and, if adopted, would permit only limited, standardized fees. As a result, the CFPB believes it is premature to conclude that any difficulties

that might have resulted from prohibiting fees for data access in the E.U. will be replicated here. As noted, the CFPB requested comment on parameters for reasonable, standardized fees that neither obstruct the access right nor impede access to interfaces. No commenters provided information in response to that request, and the CFPB does not currently have information to suggest it would be appropriate or feasible to use a standardized fee schedule to account for the wide variety of circumstances in the open banking system. The CFPB will continue to actively monitor and engage with open banking stakeholders. As the CFPB proceeds to implement this first rule under CFPA section 1033, and to ensure consumers' data rights are respected across consumer financial markets, it invites continuing input if entities believe that a regime of standardized fees along the lines of those described above is appropriate and feasible.

Data provider commenters also opposed the fee prohibition on the grounds that it would unfairly disadvantage them relative to data aggregators, which are not prohibited from charging fees to other third parties in connection with providing data they obtained through providers' developer interfaces. A few data providers, in addition to opposing it, asserted that if kept the prohibition must be accompanied by restrictions on third parties' secondary uses of covered data to ensure that the benefits of data sharing accrue to consumers, as opposed to data aggregators. These commenters argued that if the CFPB were to loosen such restrictions in the final rule then this "consumer benefit" principle would no longer apply and data provider fees to third parties should be permitted.

The fee prohibition does not unfairly advantage data aggregators relative to data providers. CFPA section 1033 describes a consumer right to access data from data providers – and gives no indication that providers may properly impinge on that right by charging for its exercise. In contrast, CFPA section 1033 does not include a right for consumers to require data

aggregators to provide covered data. Instead, the data aggregators' participation in the data-sharing process is voluntary. Fundamentally, an authorized third party's choice to use a service provider, such as a data aggregator, and a consumer's exercise of a statutory right, are entirely different things—there is no equivalence and accordingly no unfairness. Moreover, a data provider controls consumers' covered data concerning the financial product or service that the consumer obtained from the data provider, such that competitive pressures do not readily limit the data access fees that data providers might seek to charge. In contrast, data aggregators are service providers chosen by authorized third parties, who can select a different aggregator for price reasons – or connect to the data provider directly. As a result, competition should naturally put downward pressure on fees that aggregators charge third party clients.

For reasons discussed under subpart D below, the final rule does not materially increase third parties' permissible secondary uses of covered data relative to the proposal. Accordingly, it is not necessary or appropriate to permit data providers to charge fees in light of possible secondary uses that the CFPB did not propose to permit and is not permitting in this final rule. In any event, the breadth (or narrowness) of data aggregators' and other third parties' potential uses of covered data does not logically control the issue of whether data providers should be prohibited from charging fees. Competitive pressure between third parties will naturally put downward pressure on fees they are able to charge. In light of this competitive pressure, permitting data providers to charge fees would not cause the benefits of data sharing to "shift" from third parties to consumers; instead, it would cause the benefits to shift from consumers to the data providers that hold and control consumers' financial data.

Allowing cost-based fees, regardless of whether or not they are charged on a per-request basis, would not better effectuate the consumer data access right described in section 1033. The

CFPB received feedback during the SBREFA process that allowing data providers to charge fees, including fees to integrate with a developer interface, could pose a barrier to consumers' use of their data through smaller authorized third parties. *See* SBREFA Panel Report at 28. Data providers have the ability and incentive to restrict third party data access through fees and allowing data providers to charge different fees to different third parties also is likely to result in harm to consumers and third parties. *See* 88 FR 74796, 74814 (Oct. 31, 2023). In light of this, allowing data providers to charge what they see as commercially reasonable fees is likely to obstruct consumers' ability to use their data, particularly through smaller authorized third parties. In addition, as noted above, no stakeholder offered any concrete indication of a workable and administrable standard for "reasonable fees" despite the CFPB's solicitation of comment on point.[65]

3. Requirements applicable to developer interfaces (§ 1033.311)

General (§ 1033.311(a))

Proposed § 1033.311(a) stated that a developer interface required by § 1033.301(a) must satisfy the requirements set forth in § 1033.311. The CFPB received no comments objecting to this provision and the CFPB adopts it as proposed.

Standardized format (§ 1033.311(b))

Proposal

The CFPB proposed in § 1033.311(b) to require a developer interface to make available covered data in a standardized format. The CFPB proposed that the interface would be deemed to satisfy this requirement if it makes covered data available in a format set forth in a qualified

[65] It is not just the fact or level of fees that impedes consumers' exercise of statutory rights, but their potential variance as well. For example, variation in fees across data providers and variation in fees at one data provider across third parties would likely introduce material negotiating costs to third parties, thereby further impeding consumers' ability to use their data.

industry standard, or, in the absence of such a standard, if it makes available covered data 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. The CFPB preliminarily determined that this proposed requirement and accompanying safe harbors were necessary and appropriate to implement the mandate in CFPA section 1033(d) that the CFPB prescribe standards to promote the use and development of standardized formats. More specifically, the CFPB preliminarily determined that, consistent with CFPA section 1033(a) and (d), the proposal to require covered data to be made available in a usable and standardized format would reduce variation across the market and promote greater consistency of data formats. In particular, the proposed provision sought to ensure that the information systems of new-entrant and small- third parties can process covered data from the full range of data providers across the market by reducing varied formats that impel reliance on intermediaries to provide data in a usable format.

The CFPB did not propose a definition of "format," requesting comment on whether one is needed and whether the term should be defined to mean the specifications for data fields, status codes, communication protocols, or other elements to ensure third party systems can communicate with the developer interface. The CFPB also requested comment on the above safe harbors that it proposed.

Comments

All commenters, including data providers, third parties, and consumer advocates, that addressed the proposed requirement that the developer interface make available covered data in a standardized format supported it. Further, all commenters that addressed the CFPB's request for comment stated that the rule should include a definition of format and that the definition should

include, in addition to data field specifications, a data model and communication protocol for requests and responses for covered data to be exchanged.[66] Commenters stated that this broader approach to the standardized format requirement would help effectuate interoperability to support data sharing. Several data provider commenters stated that the rule should also apply its standardized format requirement to data aggregators. They argued that doing so would encourage competition and benefit consumers by facilitating the ability of an authorized third party to switch data aggregators.

Commenters' views were mixed on the CFPB's proposed approach to safe harbors for standardized formats. Commenters generally supported the proposed safe harbor for use of a standardized format set forth in a qualified industry standard, but were uncertain that one would exist by the time of the applicable compliance date for part 1033. Because of that uncertainty, commenters generally did not object to the proposed safe harbor for a widely used format, although views were mixed on that point. Specifically, some commenters expressed concern that a safe harbor for a widely used format could lead to more than one widely used format, which might not be an improvement over format differences in place today. Further, many commenters expressed concern with the CFPB's proposal that a widely used format would receive a safe harbor only in the absence of a qualified industry standard. These commenters expressed concern that this approach could make data providers reluctant to implement their developer interfaces now with a widely used format because, were they to do so and were a qualified industry standard later to adopt a different format, the providers with the widely used format would lose their safe harbor status and could feel compelled to redo their interfaces using the qualified

[66] One commenter stated that the rule's standardized format requirement should include security standards applicable to authenticating and reviewing authorization of third parties. This comment is discussed in the preamble to § 1033.331(b), which addresses how those procedures factor into the final rule.

industry standard formats. These commenters stated that the CFPB could reduce issues of multiple formats and incentivize faster deployment of developer interfaces—thereby increasing data quality and consumer safety relative to screen scraping—by working with industry participants to establish a consensus standard for data formats as soon as possible.

Final rule

For the reasons discussed herein, the CFPB is adopting final § 1033.311(b) to require a data provider's developer interface to make available covered data in a standardized and machine-readable format. The final rule also provides that indicia that the format satisfies this requirement include that it conforms to a consensus standard. The final rule defines both "format" and "standardized." Format is defined in § 1033.311(b)(1) to include structures and definitions of covered data and requirements and protocols for communicating requests and responses for covered data. Standardized is defined in § 1033.311(b)(2) to mean that it conforms to a format widely used by other data providers and designed to be readily usable by authorized third parties.

The CFPB is not providing examples of "machine-readable" file types because technology regarding automated, digital ingestion of data may evolve such that any such examples could become outdated. Section 1033.211, discussed above, defines covered data for purposes of part 1033. Section 1033.301(b), also discussed above, provides that a data provider's developer interface complies with part 1033's machine-readability requirement if it makes covered data available in a form that satisfies the requirements of § 1033.311(b). Further, as noted, § 1033.311(b) requires the developer interface to make covered data available in a format that is standardized and machine-readable and provides that indicia that the format satisfies this requirement include that the format conforms to a consensus standard.

The format definition that the CFPB is adopting gives a data provider some flexibility as to the structures and definitions of covered data made available via its developer interface so it can adapt over time to new and evolving use cases. Nonetheless, in all cases, the format must be standardized, *i.e.*, it must be widely used by other data providers and designed to be readily usable by authorized third parties. The CFPB believes that this level of flexibility is necessary and appropriate, both because, as noted, technology is rapidly evolving, and because there will inevitably be new use cases for which authorized third parties request covered data. As new uses cases develop, the best and most readily usable format for a given set of covered data could change.

For example, under § 1033.211(d) covered data includes account terms and conditions (as defined in that section), and terms and conditions include many components, some of which may be numerical and some of which may be natural language. As authorized third parties' use cases for covered data change over time, the best standardized and machine-readable format, or formats, for data providers' developer interfaces to use in making available the many components of terms and conditions will also likely change. More specifically, as authorized third parties' use cases change, the components of terms and conditions that are made available as machine-readable, discrete "callable" data fields will likely increase, and those components made available as machine-readable, lengthier "text" data fields will likely decrease.[67] Over the course of these ongoing changes in authorized third parties' use cases and pursuant to the

[67] If it is necessary for a data provider to make available a PDF file for the purpose of complying with § 1033.311(b), the PDF file should be machine-readable. While this may be possible for some PDF files, other PDF files, such as those that include covered data as images, would generally not be considered machine-readable. Section 1033.221(d), which restates the statutory exception for any information that the data provider cannot retrieve in the ordinary course of its business with respect to that information, might apply in limited circumstances when historical terms and conditions are stored as image files, as discussed in part IV.B.4 above. However, the CFPB does not expect current terms and conditions to be subject to any such exception given applicable legal requirements, as discussed with respect to § 1033.221(d) above.

"readily usable by authorized third parties" prong of the definition of "standardized" in § 1033.311(b), the CFPB expects that data providers will in good faith take reasonable steps to make the appropriate components of terms and conditions available through their developer interfaces as discrete callable data fields.

Defining format to include structures and definitions of covered data and requirements and protocols for communicating requests and responses for covered data will facilitate interoperability across data providers and third parties, including new-entrant third parties that wish to access covered data directly from data providers' developer interfaces, as opposed to through data aggregators. Interoperability is also facilitated by the two-pronged definition of standardized, under which format, to be standardized, must be both widely used by other data providers and designed to be readily usable by authorized third parties. The final rule includes a non-exhaustive list of components of format because whether a standard includes any particular component of format will depend to some degree on the standard selected.

The final rule's definition of format is necessary and appropriate to implement CFPA section 1033(a) and (d). Standardized structures and definitions of covered data and requirements and protocols for communicating requests and responses will help ensure covered data are readily made available in a usable electronic form to a wide array of authorized third parties. This facilitation of interoperability also implements the mandate of CFPA section 1033(d) that the CFPB by rule promote standardized formats for information, including through the use of machine-readable files. Without standard protocols for communicating requests and responses, data providers would forfeit the economies of scale they can achieve by making covered data available in common ways through their service providers, such as core processors, and authorized third parties would incur costs to build custom integrations to access covered data

from various data providers. These costs would undermine the benefits of requiring data providers to make available covered data in the first place. Accordingly, the § 1033.311(b) requirement to use standard protocols for communicating requests and responses for covered data is necessary and appropriate to promote the development and use of standardized formats for covered data.

The CFPB proposed that a developer interface would be deemed to satisfy the standardized format requirement if it made covered data available in a format widely used by other data providers and readily usable by authorized third parties. The CFPB believes that those attributes of a format—that it is widely used by other data providers and designed to be readily usable by authorized third parties—go directly to what it means for a format to be "standardized" and best effectuate the statute's objectives of promoting interoperability of systems to process covered data and ensuring data providers make available covered data in a usable electronic form upon request. Accordingly, the final rule adopts those attributes as components of the definition of standardized in § 1033.311(b)(2). The CFPB emphasizes that, under the definition of standardized in § 1033.311(b)(2), wide use by other data providers of a format is necessary but not sufficient for the format to qualify as standardized. For the format to qualify as standardized, the format must also be one that is designed to be readily usable by authorized third parties. This two-pronged approach—widely used by data providers and readily usable by authorized third parties—is necessary and appropriate to ensure that third parties, including in particular new-entrant and small third parties, can process covered data from a wide range of data providers across the market.

Final § 1033.311(b) makes several changes from the text of proposed § 1033.311(b)(2) to address concerns from commenters that the proposed regulatory text could have resulted in

fragmentation of data formats, and for additional clarity. The proposed provision would have deemed a format standardized in the absence of a qualified industry standard if the format is widely used by the "developer interfaces of similarly situated data providers with respect to similar data" and is readily usable by authorized third parties. The final rule replaces the phrase "similarly situated data providers," with "other data providers." This is intended to further promote the development and use of standardized data, whereas the proposed approach could have resulted in fragmentation of format standards. The final rule also omits the phrase "with respect to similar data" as superfluous because both the proposed and final regulatory text apply the standardized format requirement to "covered data." In addition, the phrase "with respect to similar data" contained in the proposed text might have inadvertently resulted in fragmentation of data formats. The final rule also omits the phrase "developer interface" as superfluous, with no change in meaning intended.

The CFPB proposed that a data provider would be deemed to satisfy the standardized format requirement if it makes covered data available in a format set forth in a qualified industry standard. In contrast, under the final rule, indicia that the standardized format requirement is satisfied include that it makes covered data available in a format set forth in a consensus standard. The CFPB is making this change—from safe harbor of compliance to indicia of compliance—because, as described above, the CFPB is defining format (which the proposal did not) to include communications protocols and requirements, as opposed to only data structures and definitions. As noted, all commenters who addressed this issue—including data providers, third parties, and consumer advocates—supported defining format and defining it in this broader way. Nonetheless, in light of this broader definition, the CFPB believes that it is possible or even likely that a given consensus standard will address only certain aspects of format as defined. As a

result, a data provider may reasonably seek to incorporate more than one consensus standard into its developer interface's systems and processes. For example, at a high level, the data provider might incorporate one standard for data structures and another for communication protocols. In addition, a given standard might have components within it that are not geared toward interoperability and therefore do not warrant safe harbor status. Accordingly, the CFPB has determined that it is more appropriate for conformance to a consensus standard to serve as indicia that the data provider's developer interface meets the standardized format requirement, rather than to serve as a safe harbor.

The change from the proposal's safe harbor approach to the final rule's indicia approach to consensus standards within § 1033.311(b) does not change the CFPB's determination that the objective of both CFPA section 1033(d) and the standardized format requirement in § 1033.311(b) is interoperability, *i.e.*, is to ensure that (1) a data provider's developer interface can expect and use a standardized data structure and communication protocol for receiving requests from and making covered data available to all third parties that request covered data through the interface[68] and (2) a third party can use and expect a standardized data structure and communication protocol for submitting requests to and receiving covered data from all data providers' developer interfaces. The CFPB does not anticipate taking action against data providers' and third parties' approach to achieving interoperability, so long as entities comply with the standardized format requirement of § 1033.311(b).

Incorporating "widely used" into the meaning of "standardized" and shifting to an approach in which a consensus standard serves as indicia of compliance (rather than a safe

[68] Consistent with § 1033.311(b), data providers may reasonably require authorized third parties to use standardized and machine-readable formats when submitting requests for covered data.

harbor) also addresses commenters' concerns that data providers might have responded to the rule as proposed by "waiting" to build their developer interfaces until a consensus standard format was adopted. Of course, the lengthening of compliance periods in the final rule provides more assurance that consensus standards will be available before compliance begins. But in any event a data provider will have certainty that its developer interface format complies with the requirement to be standardized, so long as the format is widely used by other data providers and designed to be readily usable by authorized third parties. In the event that an applicable consensus standard becomes available after the relevant compliance date, data providers can be assured of their continued compliance. They will not need to effectuate some instantaneous "redo" of the developer interface to match the consensus standard format, but, as appropriate, can simply take steps to transition to the consensus standard format in an orderly fashion.

Commercially reasonable performance (§ 1033.311(c))

The CFPB proposed in § 1033.311(c)(1) to require that performance of the interface must be commercially reasonable. All commenters who addressed the proposed requirement supported it. The CFPB has determined that the commercially reasonable performance requirement for the developer interface carries out CFPA section 1033(a) by establishing how a data provider satisfies the requirement in CFPA section 1033(a) that the data provider make covered data available in an electronic form usable by authorized third parties. The CFPB adopts the requirement, renumbered as § 1033.311(c), with technical non-substantive edits.

Response rate; quantitative minimum performance specification (§ 1033.311(c)(1))

Proposal

The CFPB proposed in § 1033.311(c)(1)(i) a quantitative minimum performance specification for a data provider's developer interface beneath which the performance of the

interface could not be commercially reasonable. Specifically, the proposed quantitative minimum performance specification was a response rate of at least 99.5 percent. The CFPB proposed to calculate the response rate as the number of proper responses by the interface divided by the total number of queries for covered data to the interface. For clarity and consistency with other provisions in part 1033, final § 1033.311(c)(1) uses "request" in lieu of "query." The CFPB neither intends nor effectuates any change to the substance of the provision as a result.

The CFPB proposed in § 1033.311(c)(1)(i)(D) to define a proper response as a response, other than any message such as an error message provided during unscheduled downtime of the interface, that meets the following three criteria: (1) the response either fulfills the query or explains why the query was not fulfilled; (2) the response is consistent with the reasonable written policies and procedures the data provider establishes and maintains pursuant to § 1033.351(a); and (3) the response is provided by the interface within a commercially reasonable amount of time. The CFPB proposed that the amount of time cannot be commercially reasonable if it is more than 3,500 milliseconds.

The CFPB proposed in § 1033.311(c)(1)(i)(A) that responses by and queries to the interface during scheduled downtime for the interface must be excluded from the calculation of the proper response rate. The CFPB also proposed in § 1033.311(c)(1)(i)(C) that the total amount of scheduled downtime for the interface in the relevant time period, such as a month, must be reasonable and in § 1033.311(c)(1)(i)(B) that in order for any downtime of the interface to qualify as scheduled downtime, the data provider must have provided reasonable notice of the downtime to all third parties to which the data provider has granted access to the interface. Finally, the CFPB proposed for both § 1033.311(c)(1)(i)(B) and (C), that adherence to a

consensus standard would be an indication that the amount and notice of downtime were reasonable.

Comments

Both third party and data provider commenters expressed certain concerns about the CFPB's proposed quantitative minimum requirements. Third party commenters generally supported the adoption of minimum quantitative performance requirements, but they saw the proposed rule as not including a broad enough set of such requirements. Those requirements it did include they described as too lax because they were below the performance levels actually being achieved in the market under third parties' extant data access agreements with data providers. They argued that the rule as proposed could unintentionally cause a race to the bottom in performance levels. More specifically, they argued that the proposed 3,500 millisecond response time was too slow and too vague. They suggested a better requirement would take the form "less than x milliseconds at least x percent of the time" and should be stricter for certain data request types, such as for authorization or account balance. Third parties also wanted quantified maximum scheduled downtimes and minimum advance notice of such downtimes.

Data provider commenters opposed the CFPB's adoption of minimum quantitative performance requirements. While not addressing current actual interface performance under their extant data access agreements, they asserted that the proposed 99.5 percent response rate would be too onerous and would impose costs without commensurate consumer benefit, particularly with respect to smaller providers that have fewer consumer account holders and that today do not have any developer interfaces. They also asserted that the proposed provisions underlying the response rate—such as downtimes, notices thereof, and 3,500 millisecond response times—were unclear and that the CFPB did not provide a sufficient factual justification for them. They

argued, for example, that the CFPB needed to provide more specificity on how to measure an interface's response time (*e.g.*, when and how to calculate the beginning and end of the response period) and on whether and how the timeframe would apply to requests for large amounts of data where transmission might take longer than the proposed 3,500 milliseconds. They argued that to the extent the CFPB purported to justify the measurements it proposed by pointing to other jurisdictions, those other jurisdictions have different factual situations and are not properly comparable for these purposes. In addition, they argued that consensus standards should have no role in interface performance requirements because standards' role has traditionally been achieving interoperability, whereas the performance requirements do not pertain to interoperability. One argued that the CFPB is effectively promoting particular technologies, in contravention of CFPA section 1033(e), by requiring specific performance standards for the developer interface. Finally, they argued that the CFPA does not provide authority to adopt the proposed quantitative specifications.

Final rule

For the reasons discussed herein, the CFPB is finalizing the quantitative minimum performance specification in proposed § 1033.311(c)(1)(i), renumbered as § 1033.311(c)(1), with certain modifications. First, the final rule does not include a numeric threshold for the time within which the interface must provide a response in order for the time to be commercially reasonable. Instead, the final rule (in § 1033.311(c)(1)(iv)(C)) requires that a proper response be provided within a commercially reasonable amount of time and that indicia that the response time is commercially reasonable include conformance to an applicable consensus standard. The CFPB adopts this approach in the final rule because the proposed 3,500 millisecond response time may not adequately take into account the variety of types and sizes of requests for covered

data that data providers' developer interfaces will receive. In addition, final § 1033.311(c)(1) requires that the response rate be equal to or greater than 99.5 percent "in each calendar month," as opposed to the proposed "relevant time period, such as a month." The CFPB makes this change for two reasons: first, to prevent a data provider from calculating its developer interface's response rate over some other time period, or varying the time period, to make appear better its interface's response rate; and second, to align the calculation time period with the calendar month disclosure time period in § 1033.341(d).

Information available to the CFPB indicates that the performance of data providers' developer interfaces is neither uniform nor always on par with what one would reasonably expect given the state of technology. Specifically, the state of technology enables consumer interfaces to operate at consistently high availability, performance, and data freshness levels, which many data providers' developer interfaces do not meet. With respect to uniformity, data from the Provider Collection indicates that providers report widely varying uptime and response time or latency measurements. This non-uniformity persists both across similarly situated providers and across the various consumer or developer interfaces a data provider may make available. *See* 88 FR 74796, 74815-16 (Oct. 31, 2023). Accordingly, the performance of data providers' developer interfaces needs both to improve and to become more consistent and predictable from where that performance is today.

The quantitative minimum 99.5 percent response rate requirement in final § 1033.311(c)(1) reflects the CFPB's determination that developer interface performance beneath that level cannot constitute commercially reasonable performance. The requirement ensures that data providers' developer interfaces perform at a sufficiently consistent and predictable level. The requirement implements CFPA section 1033(a), which requires data

providers to make covered data available in an electronic form usable by authorized third parties, and ensures consistent availability of covered data, while contemplating that limited, unscheduled downtimes may occur.

The CFPB has determined that the quantitative minimum 99.5 percent response rate is not too onerous. The minimum is in line with the results reported to the CFPB through the Provider Collection. *See* 88 FR 74796, 74816 (Oct. 31, 2023). Further, based on public comments from third parties and results reported to the CFPB through the Provider Collection and the Aggregator Collection, the minimum is below levels being achieved by larger data providers' developer interfaces today pursuant to their data access agreements with third parties. That is significant evidence that where a given data provider today has a developer interface in place, it will be reasonably feasible for the data provider's interface to continue to meet the quantitative minimum performance requirement established by § 1033.311(c)(1). It is possible over time that part 1033 going into effect will itself lead to an increased volume of data requests to larger data providers' extant developer interfaces. Nonetheless, in the CFPB's assessment, it is reasonably feasible for data providers to invest in and maintain their developer interfaces in a manner such that the increased volume does not degrade the interfaces' performance from their current levels, which, as noted, are above the quantitative minimum established in § 1033.311(c)(1). The CFPB's establishment of the 99.5 percent minimum response rate is based on the rulemaking record before it and does not rely on required performance levels in other jurisdictions. As the record demonstrates, the CFPB did consider other jurisdictions' requirements and factual situations. However, the U.S. data sharing market is differentiable from other jurisdictions (for example, the U.S. has more depository institutions than is typical in other jurisdictions) and the CFPB's legal authorities are of course specific to U.S. law. The CFPB's

determination that interface performance beneath the 99.5 percent minimum cannot be commercially reasonable appropriately reflects the rulemaking record, the U.S. data sharing market, and the CFPB's authority.

The 99.5 percent response rate minimum is below levels commonly achieved by data providers' consumer interfaces today, even for consumer interfaces maintained by data providers with no developer interface. As the CFPB noted in the proposed rule, data providers through their consumer interfaces commonly make available an amount and variety of data broader than the set of covered data that is subject to part 1033. *See* 88 FR 74796, 74816 (Oct. 31, 2023). These facts indicate that where a given data provider today has a consumer interface but does not have a developer interface, it will be reasonable for the data provider to implement a developer interface that meets the minimum performance level required by § 1033.311(c)(1). Moreover, the minimum will not apply to small depository institution data providers, because the final rule does not cover such depositories. All depository institutions subject to the final rule appear to maintain a consumer interface already and can reasonably implement a developer interface that meets the final rule's minimum performance requirements. In that regard, the final rule makes explicit that a data provider may be able to satisfy its developer interface obligation, including the 99.5 percent response rate requirement, through contract with its service provider under which the service provider screen scrapes covered data from the data provider's consumer interface and makes the covered data available to authorized third parties through a developer interface that the service provider maintains on behalf of the data provider. This type of approach can meaningfully reduce the burden of performance requirements – including the quantitative minimum – through economies of scale achieved by service providers.

The proper response definition in final § 1033.311(c)(1)(iv) underlies the required 99.5 percent response rate. The CFPB proposed (in § 1033.311(c)(1)(i)(D)) a proper response definition that excluded "any message such as an error message provided during unscheduled downtime of the interface." The final rule (in § 1033.311(c)(1)(iv)) excludes from the proper response definition "any message provided during unscheduled downtime of the interface." The CFPB neither intends nor effectuates any change to the substance of the proposed provision by omitting the clause "such as an error message." Under the final rule, as under the proposal, the proper response definition excludes any message provided during unscheduled downtime of the interface.

The proper response definition does not require in every case that covered data be returned. For example, assume a data provider has in place reasonable access caps, which comply with § 1033.311(d), limiting the frequency with which the data provider receives and responds to requests for covered data from an authorized third party through its developer interface. Assume also the data provider has in place reasonable written policies and procedures, which comply with § 1033.351(a), setting forth and describing such frequency restrictions and setting forth and describing the explanations the data provider's interface may provide for why a request to the interface was not fulfilled. Further, assume that the interface receives a request in excess of the documented reasonable frequency restrictions. Finally, assume that the interface provides a response to that request that (1) explains why the request was not fulfilled (in accord with § 1033.311(c)(1)(iv)(A)), (2) is consistent with the reasonable § 1033.351(a) policies and procedures (in accord with § 1033.311(c)(1)(iv)(B)), and (3) is provided within a commercially reasonable amount of time (in accord with § 1033.311(c)(1)(iv)(C)). That response is a proper

response under § 1033.311(c)(1)(iv) and counts favorably toward the 99.5 percent response rate set forth in § 1033.311(c)(1).

The CFPB has determined that the quantitative minimum 99.5 percent response rate in § 1033.311(c)(1) is sufficiently robust and will not result in a race to the bottom. Many smaller data providers that today do not have a developer interface will be required by the final rule to establish one. Section 1033.311(c)(1) establishes a necessary and appropriate floor for developer interface performance in these circumstances, beneath which interface performance cannot be commercially reasonable. At the same time, and particularly with respect to larger data providers, the CFPB emphasizes that the quantitative minimum is not a safe harbor. That is, it does not follow from a data provider's developer interface having met the quantitative minimum that the interface has satisfied the requirement of commercially reasonable performance established in § 1033.311(c). In addition to the quantitative minimum, § 1033.311(c)(2), discussed below, establishes indicia of what constitutes commercially reasonable performance. Those indicia include comparisons of a data provider's developer interface performance to consensus standards; to the developer interface performance of other similarly situated data providers, such as other larger data providers when the data provider is a larger data provider; and, to the performance of the data provider's consumer interface. These comparisons could indicate that a data provider's developer interface performance, and particularly a larger data provider's developer interface performance, is not commercially reasonable even if the performance meets the quantitative minimum. In other words, consideration of the indicia in § 1033.311(c)(2) could result in a determination, by an examiner for example, that a data provider's interface has not complied with the commercially reasonable performance

requirement established in § 1033.311(c) notwithstanding that the interface met the quantitative minimum in § 1033.311(c)(1).

CFPA section 1021(b) states that the CFPA's objectives include, among other things, authorizing the CFPB to exercise its authorities under Federal consumer financial law, which includes CFPA section 1033, to ensure that consumers, defined in CFPA section 1002(4) to include consumers' authorized third party representatives, are provided with timely and understandable information. In addition, the title of CFPA section 1033 indicates that its objective is to establish a consumer right to access information. The requirements of § 1033.311(c)(1) carry out these CFPA objectives by ensuring data providers respond to consumers' authorized third party representatives upon request in a manner that is commercially reasonable and that enables the representatives to access covered data in a usable electronic form. The requirements are consistent with the objective stated in CFPA section 1033(e) of not requiring or promoting a particular technology; a data provider may use any technology or technologies it wishes so long as its systems perform at the required level. Further, the rulemaking record described in part II.A establishes that data providers' competitive incentives do not align with those of authorized third parties. In light of those differing incentives, the quantitative minimum performance requirement in § 1033.311(c)(1) is necessary and appropriate to ensure covered persons do not avoid the requirement to make covered data available to authorized third parties through their developer interfaces. Beneath that minimum, performance levels would not be sufficient to enable effective realization of the CFPA's goals.

Indicia of compliance (§ 1033.311(c)(2))

Proposal

The CFPB proposed in § 1033.311(c)(1)(ii) two indicia of whether performance of the interface is commercially reasonable. The first was whether performance meets the applicable performance specifications set forth in a qualified industry standard. The second was whether the interface's performance meets the applicable performance specifications achieved by the developer interfaces established and maintained by similarly situated data providers. As with the quantitative minimum discussed above, the CFPB proposed these indicia pursuant to its preliminary determination that the performance of data providers' developer interfaces should improve over time and become more consistent and predictable. The CFPB requested comment on whether additional indicia would be appropriate and, if so, what they should be. The CFPB also requested comment on whether the final rule, instead of referring broadly to "applicable performance specifications," should name and describe certain specifications, such as the latency and uptime.

Comments

Data provider commenters opposed the indicia. They stated that the requirement of commercially reasonable performance is sufficient and appropriate in and of itself. They further argued that qualified industry standards should not serve as indicia of commercially reasonable performance because the general purpose of standards has traditionally been interoperability and the level of developer interface performance does not relate to interoperability. If qualified industry standards *were* to serve for measuring commercially reasonable performance, however, many data providers thought they should serve as a safe harbor to give providers greater compliance certainty. They also argued that the performance of similarly situated providers'

interfaces should not be among the indicia, because that would result in an ever-spiraling-upward level of required performance. Moreover, they argued that under the CFPB's proposed rule they would have no way to ascertain the performance levels of similarly situated data providers' developer interfaces because there would be no public source for that information.

Third party commenters supported the indicia. They argued that the indicia should reflect all metrics incorporated in the quantitative minimum specification in proposed § 1033.311(c)(1)(i) (discussed above), such as response rate, response time, total downtime, total scheduled downtime, and notice of downtime. They also argued that the indicia of whether the interface meets the performance level of the interfaces of other providers should be supported by a regulatory disclosure mechanism for publicly reporting all of the metrics. This disclosure requirement is discussed under § 1033.341(d) below.

Final rule

For the reasons discussed herein, the CFPB is finalizing § 1033.311(c)(1)(ii), renumbered as § 1033.311(c)(2), with modifications. Final § 1033.311(c)(2)(i) adds a third indicia: comparison to the performance of the data provider's consumer interface. As a result, under final § 1033.311(c)(2)(i), indicia that a developer interface's performance is commercially reasonable as required by § 1033.311(c) include (1) whether the interface's performance conforms to a consensus standard that is applicable to the data provider; (2) how the interface's performance compares to the performance levels achieved by the developer interfaces of similarly situated data providers; and (3) how the interface's performance compares to the performance levels achieved by the data provider's consumer interface.

The CFPB proposed in § 1033.311(c)(1)(ii) that these indicia would be based on "applicable performance specifications." In lieu of the general reference to applicable

performance specifications, final § 1033.311(c)(2)(ii) states that, for each of the above three indicia, relevant performance specifications include: (1) the interface's response rate as defined in § 1033.311(c)(1) through (c)(1)(iv) (discussed above); (2) the interface's total amount of scheduled downtime; (3) the amount of time in advance of any scheduled downtime by which notice of the downtime is provided; (4) the interface's total amount of unscheduled downtime; and (5) the interface's response time.[69]

The CFPB has determined that the specificity of final § 1033.311(c)(2), relative to the proposed rule, gives sufficient clarity to data providers for how commercial reasonability of developer interface performance will be assessed. So long as developer interfaces meet the quantitative minimum performance requirement in § 1033.311(c)(1), it is necessary and appropriate for commercial reasonability to be assessed against indicia that can take account of changing technological advancements and other factors that may bear on reasonableness in this context. By the same token, removing these indicia references altogether would result in an insufficiently robust and overly vague requirement.

It is appropriate for a consensus standard applicable to the data provider to serve as one of the three indicia of whether the performance of the data provider's developer interface is commercially reasonable. Standards bodies and the participants therein have expertise relevant to open banking issues, including but not limited to developer interface performance. The CFPB fully expects there will be give and take across industry participants in developing consensus standards for commercially reasonable developer interface performance. Consensus standards

[69] Section 1033.341(d) (discussed below) requires data providers to disclose each calendar month the response rates of their developer interfaces; nothing in part 1033 precludes data providers from reviewing such data to help them assess the commercial reasonableness of their own performance.

will serve as indicia, as relevant indicators, thereof, but will not be determinative. The CFPB believes it is appropriate for consensus standards to play this role.

It is also appropriate for the developer interface performance of similarly situated data providers to serve as the second of the three indicia. The CFPB believes that comparing interface performance to the interfaces of other providers will not result in too onerous (or unstable) a standard. Such performance is among other indicia, and does not create a requirement to be better than peer performance. But to the extent that performance lies outside that norm, that can fairly serve as indicia that performance may lack commercial reasonableness. Black's Law Dictionary defines "commercially reasonable" as "conducted in good faith and in accordance with commonly accepted commercial practice."[70] Article 4A of the Uniform Commercial Code states that the commercial reasonableness of a security procedure is to be determined by considering, among other things, "security procedures in general use by customers and receiving banks similarly situated." UCC 4A-202(c).

The performance of the data provider's consumer interface also serves appropriately as indicia of compliance. Data providers' consumer interfaces today generally achieve a level of performance that is on a par with the standards of commercial reasonability set forth in § 1033.311(c). In light of the functionality of consumer interfaces, their performance indicates that it is reasonable to expect developer interfaces to perform at similar levels. In addition, as the performance of consumer interfaces improves over time due to ongoing technological advancements, that improvement and those advancements will also indicate that it is reasonable for the performance of providers' developer interfaces to improve similarly. With these indicia, competitive pressure on consumer interface performance can also help ensure that data providers

[70] *Commercially reasonable*, Black's Law Dictionary (12th ed. 2024).

appropriately maintain the performance of developer interfaces, and do not allow that to revert to some mean below the level of commercially reasonable performance.

Access caps (§ 1033.311(d))

The CFPB proposed in § 1033.311(c)(2) to prohibit a data provider from unreasonably restricting the frequency with which it receives and responds to requests for covered data from an authorized third party through its developer interface. In other words, the CFPB proposed to permit a data provider to employ reasonable "access caps." The CFPB preliminarily determined that this would appropriately effectuate data access rights by permitting the data provider to prevent an authorized third party from unduly burdening the data provider's interface and thereby negatively impacting its ability to respond to requests from other authorized third parties. At the same time, by prohibiting *un*reasonable caps, the proposed rule would have prevented the data provider from unduly impeding the data access of that authorized third party. The CFPB also proposed that access caps must be applied in a non-discriminatory manner and consistent with the reasonable written policies and procedures that the data provider establishes and maintains pursuant to § 1033.351(a). Finally, the CFPB proposed that indicia that access caps are reasonable include that they adhere to a qualified industry standard. The CFPB requested comment on whether the final rule should differentiate between "consumer present" data requests, where the consumer is online with the third party at the time of the request, versus other requests, where the third party is refreshing the consumer's data without the consumer being online at that time.

Many commenters addressed the proposed treatment of access caps. Third party commenters generally opposed it as insufficient to prevent data providers from using such caps for pretextual reasons. They argued that a consumer is the one requesting data through an

authorized third party and that applying an access cap thereby harms the consumer. In their view, the final rule should prohibit access caps by default and require data providers to demonstrate the reasonableness of any departure from that default.

Data provider commenters generally supported the CFPB's proposal. One association representing small depository institutions argued that the CFPB should finalize the provision as proposed. Some argued, however, that data providers should have greater or total discretion to impose access caps. One questioned the CFPB's authority to impose any limit on such caps, asserting that automated batch requests from third parties do not count as consumer "requests" under CFPA section 1033(a). A few argued that qualified industry standards should have no bearing on the reasonability of an access cap, because standards to date have not played such a role.

Some third party and some data provider commenters stated that it would be appropriate for the CFPB's rule to distinguish between consumer-present requests versus other requests. These commenters stated that it would generally not be reasonable for a data provider to impose any cap on consumer-present data requests, whereas it would, or at least could, be reasonable in some circumstances for a data provider to impose such limits on other requests. Some also noted that third parties can and do address restrictions on consumer-not-present requests by, for example, submitting requests at off-peak times.

For the reasons discussed herein, the CFPB is finalizing § 1033.311(c)(2), renumbered as § 1033.311(d), as proposed, but with technical non-substantive edits for additional clarity. Reasonable access caps help ensure that requests from one authorized third party do not unduly burden the data provider's developer interface and thereby impede its ability to respond to

requests from other authorized third parties. Barring unreasonable caps remains necessary to help ensure that caps do not unduly impede an authorized third party's data access.

Under the final rule, indicia of reasonableness include adherence to a consensus standard on point. The CFPB believes that this provision will appropriately incentivize industry participants—data providers and third parties, including data aggregators—to work together towards workable standards that can take account of evolving data access technology and thereby provide a useful and enduring compliance resource. At the same time, such standards do not unduly restrict data providers because they do not represent regulatory requirements.

On the basis of its own expertise and feedback from commenters of all types that access caps on consumer-present data requests would be detrimental to consumers and to the financial products and services that consumers are using or seek to use, the CFPB observes that access caps on consumer-present data requests generally will be unreasonable and that reasonable access caps will be confined to other requests such as "batch" requests—although that confinement is not enough, alone, to make them reasonable.[71] Consumer presence indicates that the failure to provide a response promptly would have an immediate harmful effect on the consumer, especially if a consumer were enrolling in a new product or service for the first time, such that access caps would be unreasonable for this type of request, at least in the absence of some exceptional justification specific to the facts at hand. Industry participants continue to work to ensure interface availability for consumer-present requests by implementing adjustments on consumer-not-present requests. Accordingly, permitting reasonable access caps, with consensus

[71] Contrary to some commenter assertions, the CFPB has the statutory authority to address access caps imposed on consumer-not-present requests, such as batch requests. The CFPA defines "consumer" to include consumers' representatives, such as authorized third parties. That a data request comes from an authorized third party, as opposed to from an individual consumer, accordingly has no bearing on whether the submission qualifies as a "request" as that term is used in CFPA section 1033. Similarly, that section does not differentiate between batched and non-batched consumer requests for data.

standards being indicia thereof, will encourage continued industry progress toward appropriate differentiation between consumer-present and consumer-not-present requests.

Security specifications (§ 1033.311(e))

Access credentials (§ 1033.311(e)(1))

The CFPB proposed in § 1033.311(d)(1) to prohibit a data provider from allowing third parties to access its developer interface by using any credentials that a consumer uses to access the consumer interface. The proposal explained that the possession and use of consumer credentials by third parties, such as through credential-based screen scraping, raises significant security, privacy, and accuracy risks to consumers and to the market for consumer-authorized data access. For example, consumers whose credentials are exposed in a third party data breach might suffer invasions of privacy or financial harms. The proposal covered funds-storing and payment accounts, so stolen credentials could enable bad actors to cause unauthorized transactions or fraudulent use of consumers' personal financial data. The proposal also explained that credential-based screen scraping posed challenges to risk-management, including the difficulty of distinguishing legitimate from illegitimate access attempts.

The CFPB requested feedback on two specific issues. First, the CFPB asked about arrangements in which a third party procures the consumer's authority to access data, then "passes" the consumer directly to the data provider, which then authenticates the consumer using the consumer's digital banking credentials, before ultimately providing the third party with a secure access token. Second, the CFPB asked about situations in which a third party acts as both a third party and a service provider that develops and maintains a developer interface on behalf of a data provider.

Although the proposal would have prevented data providers from using credential-based screen scraping to comply with their developer interface requirements, the proposal did not explicitly state whether data providers could block screen scraping. The proposal noted that during the rule's implementation period, and for data accessed outside its coverage, the CFPB plans to monitor the market to evaluate whether data providers are blocking screen scraping without a bona fide and particularized risk management concern or without making a more secure and structured method of data access available.

The CFPB received several comments on proposed § 1033.311(d)(1). Numerous commenters compared APIs to screen scraping in discussing proposed § 1033.311(d)(1). These commenters were nearly unanimous in stating that APIs have advantages over screen scraping in accuracy, consumer privacy, and data security. For example, a trade association commenter stated that APIs are created to limit access to specifically authorized consumer data, which prevents third parties from accessing unnecessary consumer data. Other commenters stated that high-volume screen scraping can impact the availability of financial institution consumer-facing websites. However, a few credit union commenters stated that APIs introduced security risks that could allow bad actors to compromise consumers' accounts. And a community bank trade association commenter said that discouraging screen scraping in favor of developer interface requirements could violate CFPA section 1033(e)'s provision regarding "require[ing] or promot[ing] the use of any particular technology in order to develop systems for compliance."

A data aggregator commenter asked for confirmation that consumer credentials may be used in access portals that redirect consumers to enter credentials on the data provider's website. Another data aggregator commenter asked the CFPB to allow arrangements in which third parties provide information sufficient for the data provider to authenticate the consumer rather

than having data providers directly authenticate the consumer themselves. Another data aggregator commenter said that existing data access agreements that allow for credential-based access should be permitted while data providers establish their developer interfaces. A group of industry commenters and an academic institution requested clarity on whether existing data access connections would need to be re-established.

Several data providers and data provider trade association commenters asked the CFPB to authorize data providers to block screen scraping. One commenter stated that data providers should be required to take reasonable steps to prevent screen scraping once they have established developer interfaces. These commenters echoed many of the security, privacy, and accuracy risks of screen scraping discussed in the proposal. A few of these commenters asked whether data providers were obligated to permit screen scraping if their developer interfaces failed to meet the final rule's performance standards. One data provider commenter asked how data providers should treat screen scraping of non-covered data.

The CFPB is renumbering proposed § 1033.311(d)(1) as § 1033.311(e)(1) and finalizing the substance of the provision largely as proposed for the reasons discussed herein, with additional clarity regarding service providers. Final § 1033.311(e)(1) provides that a data provider must not allow a third party to access the data provider's developer interface by using any credentials that a consumer uses to access the consumer interface. Final § 1033.311(e)(1) also provides that a contract between a data provider and the data provider's service provider, pursuant to which the service provider establishes or maintains the data provider's developer interface, does not violate § 1033.311(e)(1) if the contract provides that the service provider will make covered data available, in a form and manner that satisfies the requirements of part 1033,

to authorized third parties through the developer interface by means of the service provider using a consumer's credentials to access the data from the data provider's consumer interface.

As discussed in the proposal, credential-based screen scraping creates risks to consumer privacy, accuracy, and data security, and poses challenges to data providers' systems. A core objective of the final rule is to transition the market away from using screen scraping to access covered data. Final § 1033.311(e)(1) supports this goal by preventing data providers from relying on a third party's use of consumer credentials to access the developer interface.

The CFPB disagrees with the suggestion that final § 1033.311(e)(1) risks inappropriately promoting any particular technology. Final § 1033.311(e)(1) sets forth a requirement regarding the use of consumer credentials to access the developer interface, but it allows data providers to use any technology in designing their developer interfaces.

Entities that act as service providers to data providers may, on behalf of those data providers, develop, deploy, and maintain developer interfaces whose technical specifications and requirements entail those service providers retaining and using consumers' credentials. Final § 1033.311(e)(1) does not restrict a data provider from allowing its own service provider that develops, deploys, or maintains the data provider's developer interface to use or possess consumer credentials to facilitate the provision of covered data to a consumer, even if the data provider's service provider also operates as an authorized third party. The final rule clarifies this point by stating in § 1033.311(e)(1) that a contract between a data provider and the data provider's service provider, pursuant to which the service provider maintains the data provider's developer interface, does not violate § 1033.311(e)(1) if the contract provides that the service provider will make covered data available, in a form and manner that satisfies the requirements of part 1033, to authorized third parties through the developer interface by means of the service

provider using a consumer's credentials to access the data from the data provider's consumer interface.

The central factor in analyzing various arrangements between data provider and third party for providing access through the developer interface is whether the third party uses consumer credentials to access the developer interface. For example, a third party might procure the consumer's authority to access data, then "pass" the consumer directly to the data provider, which then authenticates the consumer using the consumer's consumer interface credentials. This arrangement would not violate final § 1033.311(e)(1) because the authorized third party itself never accesses, uses, or retains the consumer's credentials. But if a third party such as a data aggregator sought to access or retain consumer credentials as a service to support access to consumer permissioned data by a variety of additional third parties, such an arrangement would violate final § 1033.311(e)(1) because the third party itself accesses and retains the consumer's credentials.

Nothing in the proposal would have precluded data providers from blocking screen scraping, and nothing in the final rule does so. However, data providers may act improperly if they attempt to block screen scraping across the board without making the requested data available through a more secure alternative. Depending on the facts and circumstances, such interference with the consumer's ability to share their personal financial data may violate the CFPA's prohibition on acts or practices that are unfair, deceptive, or abusive. However, if a data provider has established a developer interface that complies with—or in markets not yet covered by this final rule, conforms to—the requirements of this final rule, then blocking screen scraping may further consumer privacy and data security while ensuring that consumers are able to authorize access to their financial data in a manner that is safe, secure, reliable and promoting of

competition. Regarding third parties with prior arrangements that relied on credential-based access, once data providers have enabled the safe, secure, and reliable forms of data access envisioned in this rule, the CFPB cautions that screen scraping attempts by third parties to reach data covered by such arrangements could well be limited by the CFPA's prohibition on unfair, deceptive, or abusive acts or practices. 12 U.S.C. 5531.

Security program (§ 1033.311(e)(2))

Proposed § 1033.311(d)(2)(i) would have required data providers to apply to their developer interfaces an information security program that satisfies the applicable rules issued pursuant to section 501 of the GLBA, 15 U.S.C. 6801. Under proposed § 1033.311(d)(2)(ii), a data provider that is not subject to section 501 of the GLBA would have been required to apply to its developer interface the information security program required by the FTC's Standards for Safeguarding Customer Information, 16 CFR part 314. The CFPB preliminarily determined that the GLBA Safeguards Framework appropriately addresses data security risks for developer interfaces in the market for consumer-authorized financial data. The CFPB requested comment as to whether a general policies-and-procedures requirement would be more appropriate than the GLBA Safeguards Framework.

In the proposal, the CFPB noted that the GLBA Safeguards Framework generally requires each financial institution to develop, implement, and maintain a comprehensive written information security program that contains safeguards that are appropriate to the institution's size and complexity, the nature and scope of the institutions' activities, and the sensitivity of the customer information at issue. These safeguards must address specific elements set forth in the GLBA Safeguards Framework. The CFPB noted the GLBA Safeguards Framework provides a process for ensuring that such a program is commensurate with the risks faced by the financial

institution rather than a rigid list of prescriptions. The proposal noted that this flexible, risk-based approach allows the GLBA Safeguards Framework to adapt to changing technology and emerging data security threats.

Many commenters from different interest groups supported this use of the GLBA Safeguards Framework. One data provider commenter stated that the GLBA Safeguards Framework would ensure consistent data security standards for all ecosystem participants. Additionally, one consumer advocate commenter said the proposed rule would close gaps in data security coverage. On the other hand, some data provider commenters opposed the use of the GLBA Safeguards Framework on the grounds that the data providers are already subject to data security requirements. Additionally, some commenters pointed out that the FTC's Safeguards Rule was not identical to prudential regulators' Safeguards Guidelines and is not subject to FTC supervision. Specifically, commenters were concerned that the FTC lacks supervisory authority and cannot examine institutions under its jurisdiction for compliance with its Safeguards Rule.

For the reasons discussed herein, the CFPB is finalizing § 1033.311(e)(2) as proposed. As such, under § 1033.311(e)(2)(i), a data provider must apply to the developer interface an information security program that satisfies the applicable rules issued pursuant to section 501 of the GLBA, 15 U.S.C. 6801. Alternatively, under § 1033.311(e)(2)(ii), if the data provider is not subject to section 501 of the GLBA, the data provider must apply to its developer interface the information security program required by the FTC's Standards for Safeguarding Customer Information, 16 CFR part 314.

The CFPB has determined that the GLBA Safeguards Framework will best mitigate information security weaknesses within open banking transactions. The flexible nature of the Safeguards approach allows data providers some discretion in how they protect customers from

emerging threats to their data. As noted in the proposal, the FTC's Safeguards Rule includes slightly more prescriptive requirements, such as encryption, for certain elements, because the Safeguards Rule must be usable by a financial institution to determine appropriate data security measures without regular interaction with an examiner from a supervising agency.

Additionally, subjecting data providers to the GLBA Safeguards Framework is not a duplicative requirement on data providers. The Safeguards Framework allows information security programs to adapt to risks specific to the developer interface. Without this provision and its specific application to the developer interface, it is not clear consumers would have the same protection over their data across different types of data provider entities. Further, the CFPB needs to be able to adequately supervise data providers for their data security compliance. Private rules such as NACHA data security requirements or Payment Card Industry Data Security Standards require a private entity to determine what conduct complies with the rule without oversight from the CFPB. Conversely, the GLBA Safeguards Framework provides a consistent, yet flexible approach that is not dictated by a private entity.

Section 1033.311(e)(2) implements CFPA section 1033(a) by clarifying how a data provider must make available data upon request to a consumer, including an authorized third party. Establishing a consistent set of data security requirements will help ensure that developer interfaces are only making data available to consumers and authorized third parties consistent with the scope of a consumer's request and do not present unreasonable risks to the security, confidentiality, and integrity of covered data.

4. Interface access (§ 1033.321)

The CFPB proposed in § 1033.321 to clarify the circumstances under which a data provider would be permitted to block a consumer's or third party's access to its consumer or

developer interface without violating the general obligation of CFPA section 1033(a). The proposal explained that it would be inconsistent with CFPA section 1033(a) for a data provider to make available covered data to persons or entities that present unreasonable risks to the security of the data provider's safety and soundness, information systems, or consumers, or where a data provider could not take steps to ensure they are making available covered data to an actual consumer or authorized third party.

For the reasons discussed herein, the CFPB is finalizing § 1033.321 with several changes designed to clarify the operation of each paragraph, reduce the risk of unjustified denials, and reduce the burden on data providers of assessing third party risks. As discussed in greater detail below, final § 1033.321(a) generally provides that a data provider does not violate the general obligation in § 1033.201(a)(1) by denying a consumer or third party access to all elements of the interface described in § 1033.301(a) if granting access would be inconsistent with policies and procedures reasonably designed to comply with legal requirements described in § 1033.321(a)(1)(i) through (iii), and if the denial is reasonable pursuant to § 1033.321(b). Final § 1033.321(b) describes requirements that a denial must meet to be reasonable. Final § 1033.321(c) lists indicia bearing on the reasonableness of a denial pursuant to § 1033.321(b). And final § 1033.321(d) provides conditions that are each a sufficient basis for denying access to a third party.

Denials related to risk management (§ 1033.321(a))

Proposal

Proposed § 1033.321(a) generally would have provided that a data provider could deny a consumer or third party access to its consumer or developer interface based on risk management concerns. Specifically, the proposal provided that, subject to a reasonableness standard described

in proposed § 1033.321(b), a denial is not unreasonable if it is necessary to comply with the section 39 of the Federal Deposit Insurance Act or section 501 of the GLBA.

In proposing to allow data providers to deny access based on risk management concerns, the CFPB recognized that depository institutions have legal obligations to operate in a safe and sound manner, and both depository and nondepository institutions have other information security-related obligations.[72] The prudential regulators have issued supervisory guidance that sets forth risk management principles and other considerations that depository institutions can leverage when developing and implementing risk management practices. For example, in 2023 the prudential regulators issued the Interagency Guidance on Third-Party Relationships: Risk Management.[73] The proposal also recognized that consumers might suffer harm if the final rule did not allow data providers to deny a third party access to the data provider's developer interface where the data provider has legitimate risk management concerns. Indeed, the proposal stated that it would be inconsistent with CFPA section 1033(a) for a data provider to make available covered data to persons or entities that present unreasonable risks to safety and soundness or information security. At the same time, the CFPB expressed concern about risk management being used to frustrate a consumer's right to access data under CFPA section 1033, and about incentives that data providers might have to deny access. Proposed § 1033.321 was intended to accommodate these considerations.

[72] *See, e.g.*, 12 U.S.C. 1831p-1; *Interagency Guidelines Establishing Standards for Safety and Soundness*, 12 CFR part 30, app. A (OCC), 12 CFR part 208, app. D-1 (Bd. of Governors of the Fed. Rsrv. Sys.); and 12 CFR part 364, app. A (FDIC).

[73] 88 FR 37920 (June 9, 2023). *See also* Bd. of Governors of the Fed. Rsrv. Sys., FDIC, OCC, *Third-Party Relationships: A Guide for Community Banks* (May 2024), https://occ.gov/news-issuances/news-releases/2024/pub-third-party-risk-management-guide-for-community-banks.pdf; Bd. of Governors of the Fed. Rsrv. Sys, FDIC, OCC, *Conducting Due Diligence on Financial Technology Companies A Guide for Community Banks*, (Aug. 2021), https://www.occ.gov/news-issuances/news-releases/2021/nr-ia-2021-85a.pdf.

The proposal also sought to illuminate various aspects of proposed § 1033.321's operation. For example, the CFPB generally described denials of access as applicable to third parties or consumers, rather than to specific data fields requested by third parties or consumers. This was because, in the CFPB's view, third parties are in the best position to determine what covered data are reasonably necessary to provide the consumer's requested product or service. *See* 88 FR 74796, 74823 (Oct. 31, 2023). And the CFPB explained that the exceptions under CFPA section 1033, set forth in proposed § 1033.221, generally would not be appropriate for data providers to use to address risk management concerns. *See* 88 FR 74796, 74820 (Oct. 31, 2023).

The CFPB requested comment on additional ways to harmonize the risk management obligations of data providers with CFPA section 1033's data access right for consumers and authorized third parties. The CFPB also requested comment on the extent to which CFPB rules or guidance, or other sources, should address whether a data provider's denial of third party access to a developer interface under § 1033.321(a) would be reasonable with respect to any particular risk management practices.

Comments

The CFPB received numerous comments on this proposed provision. Several commenters, mostly data providers and data provider associations, said the proposal properly incorporates third party risk management principles to third party access. Many data provider commenters asserted that their prudential regulators expect a relatively high degree of vetting of third parties accessing data with consumer authorization. Several data provider commenters, and a research institute commenter, stated that third party risk management obligations applied even to third party relationships not initiated by the data provider.

Although these commenters generally supported allowing data providers to deny access to third parties, most were concerned that the proposed grounds for reasonable denials might be too narrow. For example, several data provider trade association commenters sought clarification that reasonable grounds for denying access would include concerns over fraud, reputational risk, or safety and soundness.

Some of these commenters stated that safety and soundness risks might be raised by the volume of data requested by a third party, by an unmanageable pace in onboarding third parties, or by third parties with insufficient financial resources to reimburse the data provider for unauthorized transfers. Several data providers and trade association commenters said that data providers reasonably should be able to deny access consistent with interagency guidance on third party risk management. Several commenters stated that data providers should be able to deny access based on the conduct of the third party, such as its data minimization practices, its compliance with EFTA and Regulation E, the content of its privacy policies, and its ability to manage downstream data recipients. Several commenters asked the CFPB to provide that a third party's refusal to agree to reasonable risk-related contractual terms would justify denying access. A group of data provider trade association commenters asked for guidance related to international third parties, and one trade association commenter stated that communicating denial reasons to a third party on an OFAC sanctions list might require a data provider to violate the law. A trade association commenter asked for general examples of reasonable and unreasonable denials, and a bank commenter asked for clarification that data providers may deny access to data aggregators. A bank commenter stated that the rule should clarify that the obligation on data providers to make covered data available to authorized third parties would apply only for authorized third parties domiciled in the U.S. The commenter stated that third parties that are not

domiciled in the U.S. may be subject to different privacy or data protection laws and that sharing data with such entities could undermine consumer protections and complicate risk management and liability.

Many data providers and data provider trade association commenters stated that the proposed rule appeared to contemplate a level of vetting of third parties that is infeasible. These commenters stated that data providers could be overwhelmed by the number of third parties attempting to access consumer data and would lack the resources to vet each third party to the degree required for service providers.

These commenters recommended that the final rule include various changes to reduce the burden of vetting third parties. Several data providers and data provider trade association commenters stated that the rule should provide a safe harbor for data providers who grant access to third parties making representations of their data security practices. Other data provider commenters requested safe harbor from liability for any harm caused by third parties. A few commenters stated that data providers should be allowed to negotiate data access agreements with provisions governing indemnification, insurance, and other risk-related terms. Two commenters stated that data providers should be given a reasonable period of time to vet third parties. Finally, several commenters said that the CFPB should supervise data aggregators and third parties, which would reduce the perceived risk of third parties.

In contrast, other commenters, including many third parties, and a few consumer advocates and research organizations, stated that the proposal improperly suggests that data providers should vet third parties as if they were service providers. Unlike other third party relationships, these commenters said, in the context of consumer-authorized data sharing, a third party is operating as the consumer rather than providing services to the data provider. A data

aggregator commenter stated that data providers' interests were often opposed to the interests of third parties, which incentivized denying access.

These commenters requested the final rule include additional changes designed to reduce the risk that data providers deny access on illegitimate grounds or otherwise impair consumer-authorized data access. Specifically, a research institute commenter stated that the rule should accommodate existing data access methods that are similar to the final rule's requirements so that data providers do not block them once the final rule takes effect. A few commenters recommended requiring data providers to use a standardized risk assessment method. One third party commenter stated that denials should be justified by policies and procedures that have been approved by the data provider's prudential regulator. A few of these commenters recommended prohibiting data access agreements between data providers and third parties because, they said, such agreements increase transaction costs and create inconsistent demands on third parties. Some of these commenters recommended changes related to the transparency of denials, such as requiring data providers to disclose information about their denials or the performance of their developer interfaces. Some commenters recommended changes to the process of onboarding, such as requiring data providers to operate in good faith, creating a presumption that delays in granting access of greater than two months violate the final rule, and requiring data providers to grant access once a third party has established a remediation plan for any risk identified by a data provider. Finally, a few commenters said that third parties and consumer advocates should be allowed to formally dispute any denials of access by reporting them to the CFPB.

Many types of commenters, including third parties and data providers, asked the CFPB to coordinate with the prudential regulators on risk management issues. Some of these commenters asked for guidance specific to consumer-authorized data access, while others offered specific

suggestions. Several third parties and research institute commenters stated that the CFPB and prudential regulators should clarify that risk management for authorized third parties is limited to data security or that the agencies' third party risk management guidance is inapplicable. A data provider and a trade association commenter stated that the FFIEC should identify an accreditation standard for third party information security. One bank commenter stated that the CFPB should provide guidance on risk management for data providers not subject to prudential regulation. Two commenters recommended that the agencies provide guidance stating that Regulations E and Z sufficiently address liability for any harms resulting from third party data access. Two commenters asked the CFPB and the prudential regulators to develop a process for resolving any potential conflicts between the final rule and prudential standards.

Final rule

For the reasons discussed herein, the CFPB is finalizing § 1033.321(a) with certain substantive, clarifying, and organizational changes. Final § 1033.321(a) provides that a data provider does not violate the general obligation in § 1033.201(a)(1) by denying a consumer or third party[74] access to all elements of the interface described in § 1033.301(a) if: (1) granting access would be inconsistent with policies and procedures reasonably designed to comply with: (i) safety and soundness standards of a prudential regulator, as defined at 12 U.S.C. 5481(24), of the data provider; (ii) information security standards required by section 501 of the GLBA, 15 U.S.C. 6801; or (iii) other applicable laws and regulations regarding risk management; and (2) the denial is reasonable pursuant to § 1033.321(b).

[74] Regarding comments asking whether a data provider may deny access to a data aggregator, the term "third party" is defined in the final rule to include data aggregators.

As discussed in the proposal, the CFPB recognizes that data providers have obligations regarding risk management. For example, depository institutions must operate in a safe and sound manner in compliance with applicable laws and regulations. And depository institutions and other data providers subject to the GLBA must ensure the security of the customer information that they collect and maintain. A final rule that compels data access regardless of these other legal obligations would create risks to data providers and consumers. But the CFPB also understands that data providers face some competitive incentives to deny access to third parties in ways that could threaten a consumer's right to access their data under CFPA section 1033.

The CFPB has made several changes to clarify the operation of the different elements in § 1033.321(a). First, the CFPB has revised aspects of the general standard proposed in § 1033.321(a). Specifically, the proposed rule referred to denials "based on risk management concerns" but did not specify the nature of these concerns or the meaning of denying access "based on" these concerns. Commenters also sought clarity about the relationship between the authorities cited in proposed § 1033.321(a) and the section's general term for risk management obligations.

Final § 1033.321(a) has been restructured to clarify that safety and soundness standards and information security standards are two legal requirements that might justify denying access, rather than specify an exhaustive list of grounds for denial. The CFPB has modified the proposed description of safety and soundness by removing the reference to section 39 of the Federal Deposit Insurance Act. This change reflects the fact that safety and soundness standards originate from a broader array of legal authorities and avoids implying that banks and savings associations are the only depository institutions with safety and soundness obligations. The final rule provides

these specific examples because the CFPB understands that they are especially relevant to decisions regarding third party access. But final § 1033.321(a)(2)(iii) also provides a catchall provision for other applicable laws and regulations regarding risk management to make clear that obligations regarding risk management may be found in other sources, including those raised by commenters. For example, denials may be justified by a third party's presence on a list released by OFAC, such as the Specially Designated Nationals and Blocked Persons list,[75] or by requirements to prevent money laundering and terrorist financing under the Bank Secrecy Act and the Corporate Transparency Act. *See* 31 U.S.C. 5311, 5336. This catchall provision also ensures that data providers that are not supervised by the prudential regulators are able to deny access when warranted under the rule.

In response to commenters who requested the ability to deny access using guidance issued by the prudential regulators, the CFPB has determined that denials must ultimately be grounded in legal requirements. The final rule implements consumers' data access rights in a binding, enforceable regulation. Failure to ground a denial in another legal obligation could allow non-binding, unenforceable guidance to override the final rule, which would frustrate Congress's purposes in enacting CFPA section 1033. The obligations enumerated in § 1033.321(a)(1)—safety and soundness standards, information security standards, and other laws and regulations regarding risk management—are all binding, enforceable legal requirements. However, the CFPB understands that data providers develop and apply risk management policies and procedures to support their compliance with underlying statutes and regulations, an exercise that may be informed by non-binding guidance, among other sources. To

[75] Off. of Foreign Asset Control, U.S. Dep't of Treas., *Sanctions List Service*, https://ofac.treasury.gov/sanctions-list-service (last visited Oct. 16, 2024).

reflect the role of policies and procedures and avoid excessively restricting the sources of information relevant to compliance, final § 1033.321(a)(1) refers to "policies and procedures reasonably designed to comply with" legal requirements. The CFPB assesses that these changes answer many of the questions raised by commenters regarding the types of risks covered by § 1033.321(a), whether specific references to authorities are illustrative or exhaustive, and how agency guidance relates to denial decisions.

Final § 1033.321(a)(1) also provides that a denial is justified if granting access would be "inconsistent" with policies and procedures "reasonably designed" to comply with the enumerated legal requirements. In using the term "necessary" in reference to specific statutory obligations, the proposed rule could have been read to apply a strict necessity standard to risk management obligations that a data provider might use to justify a denial. The CFPB has determined that a different approach is more appropriate to the nature of risk management. The CFPB understands that requirements to avoid unsafe or unsound practices and threats to the security of customer information generally are not defined with precision. Instead, they are evaluated based on constantly changing factual circumstances and managed by programs that are flexible enough to consider various factors.

The final rule's approach is intended to account for the flexibility and discretion that data providers exercise in designing and implementing policies and procedures regarding risk management. In the context of consumers' data access rights, the CFPB has determined that it is appropriate for data providers to exercise this discretion by attempting to grant access unless doing so would be inconsistent with reasonably designed policies and procedures. Whether a denial is the result of policies and procedures that are "reasonably designed" will depend on the circumstances. If a data provider identifies a risk that might call for denying access to a third

party, it must effectively consider how those policies and procedures can tailor any restriction on data access to the risk presented. In analyzing the extent of the risks presented by the third party, the data provider should take into account the fact that a consumer will have authorized the third party to access data, or that certain risks are mitigated by operation of part 1033. Policies and procedures would not be reasonably designed, for instance if they do not account for the protections of subpart D of this rule that address a third party's potential use of consumer-authorized data. In evaluating for whether policies and procedures are reasonably designed, the CFPB will closely evaluate whether the data provider has effectively considered how to avoid burdening the CFPA section 1033 access right while also complying with applicable laws and regulations regarding risk management. Policies and procedures will not be "reasonably designed" for purposes of § 1033.321(a)(1) if their design does not take account of whether alternative practices would be comparably effective but less burdensome to the CFPA section 1033 access right.

The final rule also separately enumerates the reasonableness element of a denial from the other requirements justifying the denial. Under final § 1033.321, a denial would have to be justified by at least one of three legal requirements provided in § 1033.321(a)(1) and would have to be reasonable pursuant to § 1033.321(a)(2). The reasonableness element in § 1033.321(a)(2) is elaborated on in § 1033.321(b), which provides requirements for reasonable denials. Final § 1033.321(a) also adds the new phrase "all elements of" the interface described in § 1033.301(a). This change better reflects the fact that denials of access under § 1033.321 involve a denial of access in its entirety. A denial would not be appropriate if it applied only to certain aspects of the developer interface, or only to certain data fields, because it would not affect "all elements" of the interface. As stated in the proposal, the CFPB has determined that

consumers and third parties are in the best position to know which covered data fields are reasonably necessary to provide a requested product or service. Similarly, a denial would not be reasonable if it were based on the volume of data a third party requested to provide the consumer's requested product or service. Concerns over the volume of data requested are appropriately addressed by final § 1033.311(d), which provides data providers flexibility regarding the frequency with which they receive or respond to requests for covered data, subject to certain limitations.

Final § 1033.321 does not require data providers to vet third parties. Instead, it recognizes that data providers will need to take account of their risk management obligations in this context. Several comments seemed premised on the existence of tension between granting third parties access to data with consumer authorization and managing risk. In general, the CFPB views data providers' risk management practices as fundamentally compatible with CFPA section 1033's data access obligations. Indeed, the final rule is designed to enable data access in a safe and secure manner, which will align the final rule with prudential imperatives. But in cases where a data provider's legal requirements regarding risk management would call for denying access, final § 1033.321 prevents data providers from having to choose between conflicting legal responsibilities.

The CFPB offers several additional points in response to comments regarding situations that might justify a denial. First, denials would be unjustified if they are based solely on a data provider's policies and procedures that override the substantive protections found in the final rule, such as asserting that the authorization procedures and obligations for third parties seeking to access covered data on consumers' behalf are insufficient. See part IV.D below. Depending on the circumstances, such a denial could be the result of policies and procedures that are not

reasonably designed under § 1033.321(a)(1), or it could be unreasonable under § 1033.321(a)(2). The final rule provides a means for consumers to effectuate their right under CFPA section 1033 to authorize access to their covered data. And the final rule contains numerous provisions that the CFPB has determined will allow consumers to realize the benefits of data access while ensuring that third parties are acting on behalf of consumers. Denying access because a third party intends to follow the final rule's protections rather than a data provider's alternative protections would infringe on a consumer's data access rights. For example, it would be unreasonable for a data provider to deny access because a third party refuses to comply with a secondary use limitation that forbids the third party from using covered data to improve the product or service the consumer requested, as permitted under final § 1033.421(c). Similarly, it would be unreasonable for a data provider to deny access because a third party's certification statement reflects the fact that it is subject to the GLBA Safeguards Rule rather than the interagency Safeguards Guidelines.

Second, the CFPB intends for final § 1033.321 to give data providers sufficient flexibility to manage the onboarding of third parties. The CFPB understands that data providers may need to onboard third parties in a staggered manner, and that failure to manage this process could incapacitate data providers' systems and the security of consumers' data. Accordingly, denying access to a third party until it can be properly onboarded may be necessary to comply with a data provider's legal obligations regarding risk management. Moreover, as described in part I, most third party access is currently achieved through the use of data aggregators. The CFPB anticipates that this arrangement will continue for the immediate future, which should reduce any implementation burden on data providers associated with the volume of third party requests.

Regarding onboarding third parties that are not domiciled in the U.S., final § 1033.321 gives data providers appropriate flexibility to deny access based on risk management obligations.

Regarding data access agreements, the final rule does not prohibit specific contractual arrangements. A blanket prohibition on such agreements would be unjustified because they may be a valid tool for managing risk. But denials based on failure to agree to certain arrangements would need to satisfy the requirements of final § 1033.321. For the same reason, the CFPB declines to create either express regulatory authorization for or prohibition against onboarding arrangements that seek third parties' assumption of particular allocations of liability. Similarly, the CFPB declines to create regulatory authorization for or prohibition against similar terms seeking specific warranties of insurance associated with such allocations. The same principles regarding denials under final § 1033.321 apply to denials in this context as well. If "required" onboarding arrangements are impermissible under final § 1033.321, a refusal to enable interface access would be improper. If such arrangements are permissible under final § 1033.321, a refusal to accept them can justify a denial of access.

Given the range of situations involving consumer-authorized data access, these principles do not yield simple one-size-fits-all requirements such as "all liabilities run with the data" or "no liability allocation can be reached in onboarding agreements." In response to the range of comments provided, however, the CFPB is providing additional guidance here as to onboarding arrangements that it considers more likely to raise concerns under § 1033.321.

First, a data provider seeking to onboard a third party to a developer interface in accordance with obligations under this rule and under applicable risk management requirements is not engaged in an arms-length commercial transaction. As a result, any exertion of market power in seeking particular terms in an onboarding arrangement will raise significant concerns

about the permissibility of a denial under § 1033.321. In this context, any arrangements not related to the effective implementation of this rule and associated risk management requirements would need to ensure they do not violate CFPA section 1033 or the anti-evasion provision of § 1033.201(a)(2).

Second, the CFPB also would have concerns under § 1033.321 if data providers demand arrangements that would effectively relieve them of their own obligations to follow the law. Such arrangements may indicate the data provider is not motivated by legal compliance, and such arrangements are likely not directly related to a specific risk presented by the third party. The potential liabilities that commenters raised, as a general matter, are provided for under applicable law, including existing law on how such liabilities may be allocated. To the extent that data providers and third parties are seeking to use onboarding arrangements to reduce the transaction costs associated with such back-end allocations, thereby lowering the systemic costs of open banking, such arrangements are less likely to raise concerns under § 1033.321. Permissibility in this context is likely to depend on whether parties are mutually attempting to reduce transaction costs, or whether one party is instead seeking to undo or change the substantive allocative outcomes that existing legal regimes would otherwise produce for the parties involved, both in terms of where law would put the loss initially and where the loss would be allocated under law.

By the same token, wholesale indemnification or "hold harmless" terms, which a number of commenters requested be imposed by or given safe harbor status under the rule, also will raise significant concerns under § 1033.321. To the extent that an indemnity seeks, effectively, to recast one party's potential liability as another's, it almost inevitably seeks to undo the substantive outcome that existing law would otherwise realize.

Third, the CFPB is particularly skeptical of, and as a result intends to carefully scrutinize for reasonableness, data provider insistence on onboarding arrangements that would allocate to third parties liability for losses associated with unauthorized transactions from accounts maintained by that data provider and where that liability arises under Regulation E.[76] Under Regulation E, financial institutions have an obligation to protect their customers against unauthorized transactions. Private network rules provide a means for financial institutions to allocate that liability. Financial institutions should continue to manage liability through appropriately developed private network rules, not one-off agreements that may manifest some improper, unilateral exertion of market power. Depositories should not use the final rule's recognition that data access onboarding needs to proceed in accordance with risk management obligations as grounds to negate the effect of their own Regulation E obligations or the need to manage liability through private network rules.

Finally, the CFPB observes that onboarding arrangements that adhere to consensus standards will carry indicia of reasonableness under § 1033.321(b).[77] For example, their development by recognized standard setters means they are likely to be directly related to a specific risk, rather than an overbroad product of a data provider's or third party's market power. The use of standard form onboarding arrangements that have been developed through the kind of processes that recognized standard setters maintain can provide an efficient model for data providers and third parties.

[76] The CFPB has the same view with respect to comments raising concerns about the allocation of any liability under Regulation Z.

[77] The presence of such onboarding arrangements might also suggest that a data provider's policies and procedures are "reasonably designed" under § 1033.321(a)(1).

Regarding comments about the potential burden on data providers of vetting third parties, the CFPB notes that final § 1033.321 does not require data providers to vet third parties. Any requirements regarding vetting are the result of data providers' existing requirements regarding risk management, such as the GLBA Safeguards Framework or safety and soundness standards. To be clear, acting on the authorization of a consumer to access their personal financial data pursuant to this final rule does not, in any way, make a third party a service provider to a data provider; and the same holds true for an aggregator with respect to its use by that third party. Authorized third parties interact with data providers for the limited purpose of accessing a consumer's covered data at the consumer's express direction, and do so within the final rule's procedural and substantive protections regarding the features of the developer interface and the collection, use, and retention of that data. This context differs from other contexts in which data providers are choosing third party business partners or service providers, or are providing data outside the safe, secure, and reliable framework that the final rule is intended to establish.

Additionally, the final rule includes various provisions designed to reduce the burden of vetting. In particular, final § 1033.321(c) allows for conformance with certain consensus standards and certifications to serve as indicia bearing on the reasonableness of a denial under § 1033.321(b), and final § 1033.321(d) lists conditions sufficient to justify a denial without the need for any further evaluation by the data provider. With respect to comments advocating CFPB supervision of data aggregators and third parties, as noted in part IV.5 above the CFPB intends to exercise its supervisory authorities in circumstances where that is appropriate. However, the CFPB's confidential supervisory process is distinct from any vetting that a data provider undertakes for its own risk management purposes.

The CFPB declines to make certain burden-related changes suggested by some commenters. Specifically, final § 1033.321 does not prescribe timing requirements applicable to denials. New timing standards would not be appropriate because final § 1033.321 is intended to work within data providers' existing processes for risk management. And the CFPB understands that risk management is an ongoing process that is difficult to reduce to a single decision point to which a deadline could be attached. Regarding liability, the CFPB declines to change the existing frameworks under Regulation E and Regulation Z for the reasons described in part IV.5 above. And the CFPB cannot create a safe harbor from data providers' existing legal obligations regarding risk management because those obligations are implemented and enforced by other agencies.

Regarding comments requesting additional changes designed to reduce the risk of improper denials, the CFPB has adopted several new indicia of reasonableness in final § 1033.321(c) that will help ensure that any denials are justified, as discussed below. These indicia, combined with the other requirements of final § 1033.321, will provide an appropriate check against improper denials. The CFPB believes that certain other suggestions are unnecessary because they are provided for elsewhere in the final rule. For example, nothing in the final rule prevents third parties, consumer advocates, or consumers from reporting denials to the CFPB or other appropriate officials, such as prudential regulators or State attorneys general. And as discussed in the analysis of final § 1033.351(b)(2), the final rule provides for transparency in denials by requiring data providers to adopt policies and procedures recording the basis for denial and communicating this basis to third parties. For commenters concerned about data providers blocking existing methods of data access before making developer

interfaces available, the CFPB has explained in the discussion of final § 1033.311(e)(1) that such attempts could constitute unfair, deceptive, or abusive acts or practices under the CFPA.

Finally, the CFPB agrees with commenters that interagency coordination is essential to the successful operation of an open banking system. Such coordination is especially important here because data providers' legal obligations regarding risk management are generally implemented and enforced by other agencies such as the prudential regulators. Accordingly, the CFPB anticipates that it will continue to work closely with other regulators to implement the rule and provide additional guidance applicable to the consumer-authorized data sharing context.

Requirements for reasonable denials (§ 1033.321(b))

Proposed § 1033.321(b) would have provided that any denials under § 1033.321 would be subject to a reasonableness standard. The proposed rule stated that to be reasonable pursuant to § 1033.321(a), a denial must, at a minimum, be directly related to a specific risk of which the data provider is aware, such as a failure of a third party to maintain adequate data security, and must be applied in a consistent and non-discriminatory manner.

A few commenters responded to proposed § 1033.321(b)'s requirement that a denial must, at a minimum, be directly related to a specific risk of which the data provider is aware. A bank and a trade association commenter asserted this condition was too narrow because, they said, data providers must anticipate potential risks that have yet to materialize. However, a data aggregator commenter said that the term "specific risk" might be overbroad if it encompasses concerns like reputational risk. A research organization requested more detail on the meaning of specific risk.

For the reasons discussed herein, the CFPB is finalizing § 1033.321(b) with certain changes for clarity about the role of this provision. Final § 1033.321(b) provides that a denial is

reasonable pursuant to § 1033.321(a)(2) if it is: (1) directly related to a specific risk of which the data provider is aware, such as a failure of a third party to maintain adequate data security; and (2) applied in a consistent and non-discriminatory manner.

Final § 1033.321(b) describes these sub-paragraphs as requirements for reasonableness rather than minimum conditions because satisfying both conditions is sufficient for a denial to be reasonable under this provision. Further guidance about the application of these requirements is found in the indicia of reasonableness are described in connection with § 1033.321(c).

The CFPB has determined that this approach provides greater clarity than the proposed use of the phrase "at a minimum," which could have implied the existence of an unknown number of unstated additional conditions. The requirements in § 1033.321(b) are designed to ensure that data providers are making denial decisions in a principled manner. The CFPB has determined that denials made in violation of these procedures carry a significant risk of being pretextual or otherwise infringing consumers' access rights under CFPA section 1033.

Final § 1033.321(b)(1) provides that a denial must be directly related to a specific risk of which the data provider is aware, such as a failure of a third party to maintain adequate data security. This requirement is designed to ensure that the concerns motivating a denial are appropriately tailored and concrete to justify denying access to a third party. The CFPB disagrees with commenters who stated that requiring data providers to articulate a specific risk would prevent them from addressing risks that have yet to materialize. Final § 1033.321(b)(1) does not require that a given harm have actually occurred before a denial is justified; only that it be articulable with specificity and based on circumstances that the data provider is aware of.

The CFPB declines to state that certain safety and soundness risks can never be stated with specificity. Final § 1033.321(b)(1) provides a procedural limit on denials of access but does

not substantively restrict the risks that a data provider may articulate. However, any denial must also be necessary to avoid being inconsistent with policies and procedures reasonably designed to comply with the legal requirements described in § 1033.321(a)(1). And final § 1033.321(c) lists indicia that can assist entities in complying with § 1033.321(b). Similarly, in response to concerns that the "specific risk" standard is insufficiently clear, the CFPB notes that it is designed to operate alongside the other provisions of this section.

Final § 1033.321(b)(1) provides that a denial must be "directly related" to a specific risk. In general, a denial is directly related to a risk if it is appropriately tailored to that risk. For example, if a data provider denies access to a third party during the onboarding process because it is missing information about that third party's information security practices, then it should grant access once it receives information that establishes the sufficiency of those practices. Under these circumstances, an indefinite denial would not be directly related to the risk justifying the denial.

Final § 1033.321(b)(2) also provides that a denial must be applied in a consistent and non-discriminatory manner. This provision is intended to ensure that data providers make similar denial decisions across third parties that present materially similar risk management concerns. As noted in the proposal, the term "non-discriminatory" in this provision carries its ordinary meaning and is not intended to refer to discrimination on a prohibited basis under Federal fair lending law.

Regarding comments recommending that the final rule require denials to be based on existing policies and procedures approved by a data provider's regulator, the CFPB believes that this comment relates to the consistency element of reasonableness. Specifically, denials based on previously adopted written policies and procedures may be more likely to be genuinely

responsive to the risks described in those policies and procedures, while denials based on newly announced concerns raise heightened risks of being unreasonable under final § 1033.321(b).

Indicia bearing on reasonableness ((§ 1033.321(c))

Proposed § 1033.321(c) provided that indicia that a denial pursuant to § 1033.321(a) is reasonable would include whether access is denied to adhere to a qualified industry standard related to data security or third party risk management. The proposal explained that conformance with an industry standard alone would not necessarily settle the question of reasonableness.

Many commenters addressed the role of standard-setting organizations or credentialing bodies. Several commenters recommended that the CFPB itself develop, or encourage the development of, an accreditation process for third parties that entitles them to data access, while others supported a registry created by a standard-setting body or by the CFPB. However, data providers and data provider trade association commenters stated that any credentialing process or consensus standard should not be dispositive. These commenters stated that risk management is specific to each third party relationship and were concerned that industry standards might conflict with the prudential regulators' standards. A few commenters stated that no standard-setting body currently has plans to issue standards related to risk management or data security. A standard-setting body commented that they do not plan to pursue authentication and data security specifications, or liability determinations.

Other commenters recommended that the final rule include additional factors relevant to a denial of access. One data aggregator commenter recommended creating a presumption in favor of access for third parties that attest to following appropriate data security standards. This commenter also suggested including indicia of unreasonable denials for denials made despite a third party certifying to the adequacy of its security measures or conforming to an accreditation

developed by the CFPB or a standard setting body. A trade association commenter recommended that the final rule give conclusive weight to similar factors related to unreasonable denials, such as certification by the third party, conformance to an industry standard, or supervision by a regulatory agency.

For the reasons discussed herein, the CFPB is finalizing § 1033.321(c) with several new indicia bearing on the reasonableness of a denial under § 1033.321(b). Final § 1033.321(c) states that indicia bearing on the reasonableness of a denial under § 1033.321(b) include: (1) whether the denial adheres to a consensus standard related to risk management; (2) whether the denial proceeds from standardized risk management criteria that are available to the third party upon request; and (3) whether the third party has a certification or other identification of fitness to access covered data that is maintained or recognized by a recognized standard setter or the CFPB.

The indicia listed in final § 1033.321(c) include factors that the can further guide compliance with § 1033.321(b). The indicia do not serve as conclusive evidence or presumptions of compliance because the CFPB understands that the circumstances surrounding a denial may render it unreasonable or reasonable for purposes of § 1033.321(b) despite the presence or absence of these indicia. For example, a third party might possess a certification regarding the adequacy of its information security program, but a data provider might nevertheless reasonably deny access if it discovers deficiencies in that program such that providing access would be inconsistent with policies and procedures reasonably designed to comply with a legal requirement regarding risk management.

Final § 1033.321(c)(1) largely restates the proposal's indicia related to qualified industry standards, with changes to conform to the final rule's use of the term "consensus standard" and

§ 1033.321's use of the term "risk management" to capture various legal obligations related to safe and sound practices, information security, and similar applicable statutory or regulatory obligations. A denial made according to a consensus standard may be likely to be reasonable because it reflects a consistent set of standards developed with the participation of a variety of stakeholders, including data providers and third parties. The CFPB believes this provision will promote safe and competitive third party access.

Final § 1033.321(c)(2) relates to whether the denial proceeds from standardized criteria regarding risk management available to the third party upon request. The CFPB agrees with commenters about the value of a standardized risk assessment method. Denials made according to standardized, knowable criteria may be likely to be reasonable because they are the product of a principled decision-making process. At the same time, the CFPB recognizes that in rare cases a data provider might face an unanticipated risk that justifies denying access. Additionally, there may be aspects of a risk management policy that would undermine the policy's effectiveness if disclosed to a third party. For that reason, final § 1033.321(c)(2) is among the indicia of reasonableness rather than a requirement of reasonableness.

Final § 1033.321(c)(3) relates to credentials or other identifications of fitness to access covered data. The CFPB agrees with commenters who stated that a credentialing or registry system could serve a useful role in the open banking system. But the CFPB also recognizes that such a credential could not supplant data providers' risk management obligations. Such credentials would reduce both the burden of vetting and the risk of unreasonable denials under § 1033.321(b). A denial of a credentialed third party may be likely to be unreasonable under § 1033.321(b) because, among other things, the third party has presented evidence of its fitness to access covered data, supported either directly or indirectly by a relevant regulator. Conversely,

a denial of a noncredentialled third party may be likely to be reasonable under § 1033.321(b) if such credential were customary among third parties. Final § 1033.321(c)(3) allows for a broad range of credentials to serve as indicia, including lists of approved third parties, and for a broad range of entities that may produce or validate such a credential.

The CFPB acknowledges comments stating that no consensus standard or credentialing entity relevant to denials is likely to exist in the immediate future. Regarding comments requesting standards or entities directly approved by the CFPB, the CFPB believes that these measures would be most effective and efficient if done on a coordinated basis with other regulators. Final § 1033.321(c)(3) does not commit the CFPB (or other regulators) to recognizing such a credential or credentialing entity. But given the interest commenters expressed in this type of accreditation, the CFPB believes that developments in this direction would promote consistent and non-discriminatory practices with respect to managing third party data access. Therefore, final § 1033.321(c)(3) accommodates the creation of such standards or entities.

The CFPB believes the indicia provided in final § 1033.321(c) incorporate many of the suggestions made by commenters for improving the efficiency of third party data access. The CFPB declines to adopt all suggested indicia because the final rule prioritizes indicia the CFPB believes are likely to be most relevant and impactful to evaluating the reasonableness of a data provider's denial under § 1033.321(b). Final § 1033.321(c) is not an exhaustive list of factors that can guide compliance with § 1033.321(b).

Conditions sufficient to justify a denial (§ 1033.321(d))

The CFPB proposed in § 1033.321(d)(1) to clarify that a data provider would have a reasonable basis for denying access to a third party under § 1033.321(a) if the third party does not present evidence that its data security practices are adequate to safeguard the covered data,

provided the denial of access is not otherwise unreasonable. The CFPB explained that this provision was intended to alleviate the concerns related to the potential burden of vetting on smaller data providers because if the third party does not present such evidence, the data provider may deny access without vetting the third party.

The CFPB proposed in § 1033.321(d)(2) to clarify that a data provider would have a reasonable basis for denying a third party access if the third party does not make public certain information about itself. This information consisted of data that the CFPB believed would benefit the efficiency of the open banking system, such as the third party's legal name and any assumed name it is using when doing business with the consumer, a link to its website, and its LEI. Proposed § 1033.321(d)(2) would have also permitted the data provider to deny access if the information was not made available in both human-readable and machine-readable formats, and if the information is not readily identifiable to members of the public (meaning the information must be at least as available as it would be on a public website).

The CFPB requested comment on whether to specify the types of evidence a third party would need to present about its data security practices that would give a data provider a reasonable basis to deny access, and what types of evidence might provide such a basis. The CFPB also requested comment on whether developing an accreditation system could reduce diligence costs for both data providers and third parties and increase compliance certainty for data providers, and on the steps necessary to develop such a credential and how the CFPB or other regulators could support such efforts.

The CFPB also requested comment on whether it should indicate that conformance to a specific standard or a qualified industry standard would be relevant indicia for a third party's machine-readability compliance; whether it should issue regulations or guidance that would

make it easier for data providers and other members of the public to identify a particular third party's information; whether it should provide that a data provider is permitted to deny access if the third party does not submit to the CFPB the link to the website on which this information is disclosed; and whether data providers should have to provide information or notice to the CFPB regarding their procedures and decisions to approve or deny third parties for access to their developer interfaces.

Several commenters addressed proposed § 1033.321(d)(1). Several commenters, including third parties, research organizations, and consumer advocates, commented that the final rule should identify the types of evidence that would establish the adequacy of a third party's data security practices. Types of evidence suggested by these commenters typically included a credential issued by an independent entity or an industry standard provided by a standard-setting body. These commenters differed on whether such evidence should be dispositive. One trade association said that the CFPB should not specify the types of evidence that would establish that a third party's data security practices are adequate.

The CFPB also received several comments on proposed § 1033.321(d)(2). A bank commenter stated that the rule should not require a third party to provide a phone number that any outside party could use to inquire about security practices because doing so might compromise the third party's security. A consumer advocate commenter said that any directory should include only approved third parties to prevent public confusion. Regarding the LEI, one commenter stated that the LEI could be used to identify a third party's legal name, while another commenter said that an LEI was useful but not sufficient for verifying a third party's identity. A data aggregator commenter asserted that because many third parties currently lack LEIs and the

process for obtaining one was difficult, the final rule should also permit third parties to use alternative identifiers such as a tax identification number or employer identification number.

For the reasons discussed herein, the CFPB is finalizing § 1033.321(d) with certain organizational and clarifying changes to improve the function of this provision in the broader context of § 1033.321. Final § 1033.321(d)(1) provides that each of the following is a sufficient basis for denying access to a third party: (1) The third party does not present any evidence that its information security practices are adequate to safeguard the covered data; or (2) The third party does not make the following information available in both human-readable and machine-readable formats, and readily identifiable to members of the public, meaning the information must be at least as available as it would be on a public website: (i) Its legal name and, if applicable, any assumed name it is using while doing business with the consumer; (ii) A link to its website; (iii) Its LEI that is issued by: (A) A utility endorsed by the LEI Regulatory Oversight Committee, or (B) A utility endorsed or otherwise governed by the Global LEI Foundation (or any successor thereof) after the Global LEI Foundation assumes operational governance of the global LEI system; and (iv) Contact information a data provider can use to inquire about the third party's information security and compliance practices.

Final § 1033.321(d) is intended to reduce burden on data providers by listing conditions that, if met, justify denying access without expending any further resources on vetting a third party. Accordingly, final § 1033.321(d)(1) clarifies that a denial is justified if a third party does not present "any" evidence of the adequacy of its information security practices. As proposed, the CFPB believes that this provision could have been read to require third parties to present a certain type of evidence regarding their information security practices that would entitle the third party to access consumer data. Understandably, many commenters focused on the kinds of

evidence that could satisfy such a requirement. Many of these commenters discussed credentialling functions and consensus standards, and the CFPB has reflected this feedback in finalizing indicia related to this evidence in § 1033.321(c)(1) and (3). But the CFPB's intent for final § 1033.321(d)(1) is more limited. It is designed as a means of streamlining the vetting process by clarifying that data providers may deny third parties that failed to clear the minimum bar necessary for data providers to evaluate the third party's practices. Such evidence might take different forms, including a third party's policies and procedures, or audits or reports. But if a third party cannot present any evidence that its information security practices are adequate, then a data provider may deny access without additional investigation.

Final § 1033.321(d)(2) lists certain information that a third party must make available. As explained in the proposal, the CFPB finds that this information will aid the efficiency of the open banking system by helping data providers authenticate the identities of third parties and facilitating any outreach to the third party that may be required as part of the data provider's due diligence. The information required by final § 1033.321(d)(2) is largely the same as the information the CFPB proposed, with a minor change. Specifically, to avoid implying that data providers absolutely may not inquire about topics other than information security, final § 1033.321(d)(2)(iv) describes a third party's contact information as information a data provider can use to inquire about the third party's information security "and compliance" practices. The CFPB disagrees that such disclosing such contact information might compromise a third party's security. The final rule does not require disclosing any substantive information about a third party's information security program.

The CFPB declines to add alternative identifying information other than the LEI, such as tax identification number or employer identification number. An LEI allows users to link an

entity to its corporate family, which improves data providers' ability to identify the third party seeking access. Additionally, the CFPB has not found that LEIs are unduly burdensome to obtain in its experience administering the Home Mortgage Disclosure Act and Small Business Lending rules, both of which require financial institutions to report an LEI.

5. Responding to requests for information (§ 1033.331)

Responding to requests—access by consumers (§ 1033.331(a))

The CFPB proposed in § 1033.331(a) to prescribe the conditions that apply when consumers are seeking covered data. Under proposed § 1033.331(a), to comply with proposed § 1033.201(a), upon request from a consumer, a data provider would be required to make available covered data when it receives information sufficient to: (1) authenticate the consumer's identity and (2) identify the scope of the data requested. The CFPB explained that proposed § 1033.331(a) is not a requirement to authenticate the consumer's identity and identify the scope of the data requested. Rather, proposed § 1033.331(a) identifies the point in time that a data provider must respond to the request. The CFPB received limited comments on this provision. Several commenters asked that the CFPB clarify how data providers may verify consumers' identities when consumers access information under the rule.

For the reasons herein, the CFPB is finalizing § 1033.331(a) as proposed with an updated cross-reference. Section 1033.331(a) carries out the objective of CFPA section 1033(a) for data providers to make covered data available upon request to a consumer by defining what information triggers a data provider's obligation to make covered data available to a consumer. As noted in the proposal, these conditions would be satisfied through procedures in use by most consumer interfaces today. With regard to the comments requesting clarification on how a data provider may verify a consumer's identity for purposes of § 1033.331(a), the CFPB notes that

the only requirement in the rule related to how a data provider must authenticate a consumer's identity is the requirement at § 1033.311(e)(2) with respect to the GLBA Safeguards Framework.

Responding to requests—access by third parties (§ 1033.331(b))

Conditions that apply to requests from third parties (§ 1033.331(b)(1))

Proposal

Under proposed § 1033.331(b)(1), a data provider would have been required under § 1033.201(a) to make available covered data to a third party, when it receives certain information described in § 1033.311(b)(i) through (iv). The CFPB proposed in § 1033.331(b)(1)(i) that a data provider would need to receive information sufficient to authenticate the consumer's identity. The CFPB explained that before a data provider grants a third party access to covered data today, the consumer is typically redirected from a third party's interface to the data provider's interface to authenticate the consumer's identity, usually by providing account credentials. Where consumers provide their credentials directly to the data provider through such an interface, the data provider would generally receive information sufficient to authenticate the consumer's identity for purposes of proposed § 1033.331(b)(1)(i).

Under proposed § 1033.331(b)(1)(ii), the data provider would need to receive information sufficient to authenticate the third party's identity. The CFPB explained that an example of such information would include an access token obtained by the third party that has been approved to access the data provider's interface. Under proposed § 1033.331(b)(1)(iii), a data provider would need to receive information sufficient to confirm the third party has followed the authorization procedures in proposed § 1033.401. The CFPB explained that 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.

Finally, under proposed § 1033.331(b)(1)(iv), a data provider would need to receive information sufficient to identify the scope of the data requested. The CFPB explained that in certain situations, the scope of information requested by an authorized third party might be ambiguous. In these situations, under proposed § 1033.331(b)(1)(iv), a data provider could seek to clarify the scope of an authorized third party's request with a consumer. For example, the CFPB explained that there might be circumstances in which a data provider could seek to clarify whether a consumer intended to consent to share information from particular accounts or particular types of information not specified in the consumer's third party authorization.

The CFPB requested comment on the potential for technology to evolve such that a data provider could satisfy appropriate data security and other risk management standards without receiving a consumer's account credentials directly from the consumer. The CFPB also requested comment on whether clarifications are needed regarding what information would be sufficient to confirm the third party has followed the authorization procedures in the context of automated requests received through a developer interface. Finally, the CFPB requested comment on whether additional clarifications or procedures are needed to ensure a data provider does not design its developer interface to receive information sufficient to satisfy the conditions set forth in proposed § 1033.331(b)(1) but in a way that frustrates the ability of authorized third parties to receive timely responses to requests for covered data.

Comments

A consumer advocate commenter supported the proposed conditions in § 1033.331(b)(1) for data providers to verify a third party's authorization to access consumer data and authenticate the identity of third parties before they make available covered data. However, this commenter, along with others, seemed to interpret proposed § 1033.331(b)(1) as setting forth strict

requirements, as opposed to conditions that define the trigger for when a request must be responded to by a data provider, which data provider commenters were concerned would be overly burdensome with respect to confirming a third party's authorization. This concern was twofold: (1) data providers would not have actual knowledge of how the third party received authorization, which they suggested could have been gathered through unfair, deceptive or abusive third party authorization procedures; and (2) confirming that every authorized third party complied with the authorization procedures would be resource-intensive. Further, bank commenters that interpreted the provision to be an obligation were generally unclear as to what was required of them to authenticate the consumer or third party or to confirm the third party followed the proposed § 1033.401 authorization procedures.

Bank commenters offered a number of suggestions for revisions. Some bank commenters recommended that the CFPB modify the regulatory text in proposed § 1033.331(b)(1)(iii) to clarify that a data provider has the right but not the obligation to "confirm the third party has followed the authorization procedures in § 1033.401." One bank trade association commenter recommended that the CFPB change the "confirm" language in proposed § 1033.331(b)(1)(iii) to "reasonably confirm," arguing that this would give data providers more discretion to determine whether the third party authorization actually represents the "consumer's express informed consent" as required by proposed § 1033.401(c). At least one bank commenter understood proposed § 1033.331(b) as setting forth requirements applicable every time a third party requests data from the developer interface, even where the consumer had authorized the third party to access data multiple times within an extended duration. In such cases, one data provider trade association commenter recommended that the CFPB distinguish between initial requests in which an authorization is first presented to the data provider, and subsequent requests that were

authorized under the initial request. The commenter stated that this would give data providers more flexibility with respect to reviewing subsequent requests. Specifically, the commenter suggested that data requests by authorized third parties relying on an existing, unchanged authorization should not require additional authentication by the data provider.

Third party commenters were generally concerned that data providers could unduly delay the processing of requests to promote the data provider's own product or service. One third party commenter suggested the final rule state that a data provider should provide a prompt response to legitimate requests by third parties. This commenter explained that some data providers have purposefully frustrated request procedures by ignoring requests to discuss API access or by misconstruing their direct data connection.

Final rule

For the reasons discussed herein, the CFPB is finalizing § 1033.331(b)(1) with a minor change for clarity and an updated cross-reference. Section 1033.331(b)(1) carries out the objective of CFPA section 1033(a) for data providers to make covered data available upon request to a consumer by defining what information triggers a data provider's obligation to make covered data available to a third party purporting to be authorized to act on behalf of a consumer. Under § 1033.331(b)(1), to comply with the requirements in § 1033.201(a)(1), upon request from an authorized third party, a data provider must make available covered data when it receives certain information. This information consists of: information sufficient to authenticate the consumer's identity under § 1033.331(b)(1)(i); information sufficient to authenticate the third party's identity under § 1033.331(b)(1)(ii); information sufficient to document the third party has followed the § 1033.401 authorization procedures under § 1033.331(b)(1)(iii); and information sufficient to identify the scope of the data requested under § 1033.331(b)(1)(iv).

Consistent with the proposal, § 1033.331(b)(1) does not impose obligations on data providers to obtain certain information prior to responding to a request for covered data. Rather, § 1033.331(b)(1) sets forth the trigger for when a data provider is obligated to make covered data available to an authorized third party pursuant to the rule. Section 1033.331(b)(1) does not by its terms require a data provider to authenticate consumers or third parties, or confirm authorizations of third parties. However, the CFPB expects data providers generally will do so to ensure they are responding to consumers' requests and to comply with the GLBA Safeguards Framework (consistent with § 1033.311(e)(2)), any safety and soundness requirements, and other legal obligations, such as the CFPA prohibition against unfair, deceptive, or abusive acts or practices, as applicable. In particular, the CFPB does not believe § 1033.331(b)(1)(iii) imposes significant burden with respect to how a data provider processes information about a third party's compliance with the rule's authorization procedures. The CFPB has determined that data providers should not be responsible for obtaining a consumer's authorization for a third party because third parties are in the best position to determine what data elements are reasonably necessary. However, § 1033.331(b)(1)(iii) does not require a data provider to independently verify the third party has followed each of the § 1033.401 authorization procedures, but instead describes a condition in which the data provider receives information sufficient to document such authorization. As discussed in the proposal, receipt of a copy of the signed authorization disclosure should constitute information sufficient to confirm third party authorization, absent facts to the contrary. However, in light of comments, the CFPB appreciates that the use of "confirm" in proposed § 1033.331(b)(1)(iii) could suggest a rigorous due diligence obligation. Accordingly, the final rule uses "document" rather than "confirm" to clarify the nature of § 1033.331(b)(1)(iii).

In response to bank commenter questions about whether any particular method of authentication is necessary or sufficient, the final rule does not so specify. The final rule only requires data providers to satisfy the data security requirements in § 1033.311(e) regarding the use of consumer credentials and compliance with the Safeguards Framework. The CFPB believes the Safeguards Framework is sufficiently clear that data providers must take some reasonable steps to authenticate who is accessing the data, and the CFPB does not believe it is necessary to prescribe a single means of authentication in the final rule. The final rule does not preclude a data provider from applying different treatment to initial and subsequent data requests covered by the same authorization, if otherwise permissible under § 1033.311(e). The CFPB notes that standard-setting bodies have created standards in this space and consensus standards could be useful to demonstrating whether a trigger has been met. Accordingly, indicia that bear on whether a trigger in § 1033.331(b) has been met include conformance to a consensus standard.

Third party commenters affirmed the concern identified by the CFPB in its request for comment that a data provider could frustrate the ability of authorized third parties to receive timely responses to requests. As discussed in detail above, final § 1033.201(a)(2) includes an anti-evasion provision limiting data providers' ability to frustrate an authorized third party's receipt of covered data. To illustrate how § 1033.201(a)(2) applies to § 1033.331(b), the rule includes an example of conduct that violates the anti-evasion provision in the context of requests, as discussed below with respect to § 1033.331(b)(2) below. The CFPB has determined the anti-evasion provision can more flexibly address the variety of conduct that could interfere with requests than more detailed procedural requirements.

A third party's authorization could extend to multiple requests, depending on the duration and frequency of access authorized by the consumer. As noted in the proposal, data providers today often issue third parties accessing their systems a token that can be presented for subsequent requests covered by a single authorization. If the data provider adequately designs its developer interface, review of the initial request by the third party should give the data provider adequate opportunity to obtain evidence of the third party's authorization including, if appropriate, confirmation by the consumer. In general, it should not be necessary to keep confirming the third party's authorization with the consumer in connection with each previously authorized request. If a data provider continues to request this information, then the data provider will raise concerns about interfering with the access right, in violation of the anti-evasion provision in § 1033.201(a)(2).

Confirmation of third party authorization (§ 1033.331(b)(2))

The CFPB proposed in § 1033.331(b)(2) that a data provider would be permitted to confirm the scope of a third party's authorization to access the consumer's data by asking the consumer to confirm (1) the account(s) to which the third party is seeking access and (2) the categories of covered data the third party is requesting to access, as disclosed by the third party pursuant to proposed § 1033.411(b)(4). The proposed rule explained that data providers might need to confirm the account(s) to which the third party is seeking access because that information might not be clear from the authorization disclosure, such as where a consumer has multiple accounts. Additionally, the proposed rule explained that permitting the data provider to confirm the categories of covered data would give the consumer an opportunity to review what data they would be authorizing and give data providers greater certainty that the consumer has authorized the request. The proposed rule requested comment on whether the final rule should

instead permit data providers to confirm § 1033.331(b)(2) information with the consumer only where reasonably necessary.

In general, bank commenters supported proposed § 1033.331(b)(2). One consumer advocate commenter said the CFPB should require, rather than permit, the data provider to send a confirmation to the consumer when it receives a third party request. Third party commenters opposed proposed § 1033.331(b)(2) on the grounds that it would cause undue friction in the data access process and suggested certain revisions. For example, one third party commenter recommended that data providers not be allowed to confirm an authorization if the third party transmits a record of the consumer's account selection. Another commenter noted that the proposal did not set forth a requirement for how or how quickly the data provider confirm third party authorization, and noted that an anticompetitive data provider could decide to confirm each request via certified mail. Additionally, some third party commenters recommended that the CFPB revise proposed § 1033.331(b)(2) to require data providers to collect account confirmation via the developer interface and not from the consumer.

The CFPB is finalizing § 1033.331(b)(2) as proposed and has added an example to address concerns raised by commenters about interference by data providers, as discussed below. Section 1033.331(b)(2) carries out the objective of CFPA section 1033(a) by clarifying that data provider is permitted to take certain steps to confirm the scope of information requested by a third party purporting to be authorized to act on behalf of a consumer. Allowing data providers to confirm authorizations directly with the consumer, as described in § 1033.331(b)(2)(i) and (ii), can reduce the risk of unintended or fraudulent authorizations and may be a necessary part of data providers' risk management program. However, requiring data providers to obtain consumer confirmation in every case could impose an undue burden on the data provider and the access

right, especially in light of the protections in § 1033.311(e)(2) and data providers' other applicable legal obligations. In response to third party commenters' suggestions for alternative procedures to obviate the need for data providers to confirm authorization, it is not clear that it would be feasible to require data providers to transmit records of consumers' accounts to third parties before a third party has initially requested access to covered data.

While data providers are permitted to confirm authorizations with consumers pursuant to § 1033.331(b)(2)(i) and (ii), data providers must avoid interfering with the statutory access right pursuant to § 1033.201(a)(2). As discussed above with respect to § 1033.331(b)(1), a data provider will create risks of violating the anti-evasion provision at § 1033.201(a)(2) if it seeks reconfirmation with consumers after it has already documented the third party's authorization to access covered data. In response to commenter concerns about undue friction introduce by data providers, the final rule includes an example that illustrates how a data provider would violate § 1033.201(a)(2) if a data provider knows or should know its confirmation procedures would be likely to prevent, interfere with, or materially discourage access to covered data.

Covered data not required to be made available (§ 1033.331(c))

Proposed § 1033.331(c) stated that, notwithstanding § 1033.331(a) and (b) (*i.e.*, the general triggers for making covered data available in response to consumer or third party requests), a data provider is not required to make covered data available in response to a request in four circumstances: if the data are withheld because an exception described in § 1033.221 applies (§ 1033.331(c)(1)); if the data provider has a basis to deny access pursuant to risk management concerns in accordance with § 1033.321(a) (§ 1033.331(c)(2)); if its interface is not available when the data provider receives a request, although the performance specifications at § 1033.311 would still apply (§ 1033.331(c)(3)); or if the request is for access by a third party

but the consumer's authorization is not valid for one of three reasons: (1) the consumer has revoked the third party's authorization pursuant to proposed § 1033.331(e); (2) the data provider has received notice that the consumer has revoked the third party's authorization pursuant to proposed § 1033.421(h)(2); or (3) the consumer has not provided a new authorization to the third party after the maximum duration period, as described in proposed § 1033.421(b)(2) (§ 1033.331(c)(4)). The CFPB requested comment on whether additional clarification was needed to reduce the opportunity for data providers to deny requests without justification under the proposed provision.

One consumer advocate suggested limiting the scope of § 1033.331(c)(1) by narrowing the scope of the exceptions under § 1033.221(a) and (d), discussed above in part IV.B.4. The commenter asserted fewer exceptions to the requirement that data providers make information available make it more transparent to consumers how data providers use their data. Several data provider commenters recommended that final § 1033.331(c) clarify that failure to meet the conditions in § 1033.331(a) and (b) does not require a data provider to make covered data available in response to a request. Further, some bank commenters suggested that small data providers would be overburdened by what they interpreted as a requirement under proposed § 1033.331(c) to track all individual authorization and access requests.

For the reasons discussed herein, the CFPB is finalizing § 1033.331(c) with certain revisions. Final § 1033.331(c) lists five circumstances under which a data provider is not required to make covered data available in response to a request. The final rule adopts § 1033.331(c)(1), (3), and (4) as proposed. As discussed below, final § 1033.331(c)(2) now lists the circumstance in which data are not in the data provider's control or possession, consistent with the requirement in § 1033.201(a)(1). Also as discussed below, the final rule also includes

new § 1033.331(c)(5), which describes the circumstance in which the data provider has not received information sufficient to satisfy the conditions in § 1033.331(a) or (b), with conforming changes to the first sentence of § 1033.331(c). The final rule also revises the title to paragraph § 1033.331(c), from "Response not required," to "Covered data not required to be made available." The final language more accurately reflects the operation of the rule because certain responses are required even if covered data are not available, pursuant to policies and procedures required under § 1033.351(b). Section 1033.331(c) carries out the objective of CFPA section 1033(a) for data providers to make covered data available "upon request" by clarifying when a data provider is not required to make data available in response to a request.

Proposed § 1033.331(c)(2) would have stated that a data provider is not required to respond to a request when the data provider has a basis to deny access pursuant to risk management concerns in accordance with proposed § 1033.321(a). As discussed in the proposal, proposed § 1033.321 was intended to apply to a consumer's or third party's access to the interface as a whole, rather than access to specific data fields requested. In terms of the operation of § 1033.331, where a third party that previously had been granted access to an interface is subsequently denied access pursuant to § 1033.321, the data provider would be denying the request because it could not authenticate the third party's identity pursuant to § 1033.331(b)(1)(ii). Consistent with the purpose of the clarification in final § 1033.321(a) that data providers can deny a consumer or a third party access to "all elements" of the interface, the CFPB is revising final § 1033.331(c) to treat a denial by operation of § 1033.321 as a failure to authenticate under § 1033.331(a) or (b). For these reasons, the CFPB is not adopting § 1033.331(c)(2) as proposed. This change does not alter the operation of § 1033.321 that was intended by the proposal. In place of the text in proposed § 1033.331(c)(2) regarding § 1033.321,

the final rule includes new § 1033.331(c)(2) to specify a circumstance that had not been identified in the proposal but that nonetheless would justify a denial of information requested: when the data are not in the data provider's control or possession, consistent with the general requirement in § 1033.201(a)(1). This change is intended to clarify the operation of the rule as a whole, rather than identify a new basis that a data provider could deny a request.

Additionally, the final rule includes new § 1033.331(c)(5) in response to comments requesting clarification that § 1033.331(a) and (b) do not require a data provider to make covered data available in response to a request. The CFPB agrees with commenters that this addition would facilitate compliance by clarifying the operation of the rule. The general conditions that trigger a data provider's obligation to make covered data available are set forth in § 1033.331(a) with respect to consumer requests and § 1033.331(b) with respect to third party requests. A data provider would not be required to make information available if those conditions were not met. The proposed rule did not list those explicitly as bases under § 1033.331(c), but generally explained that a data provider would not be required to make covered data available in response to a request as set forth in paragraphs (c)(1) through (4) "[n]otwithstanding the general rules in § 1033.331(a) and (b)." The CFPB believes that identifying these bases more directly will better facilitate compliance with the rule, including with respect to § 1033.351(b)(3), discussed below in part IV.C.7. Thus, final § 1033.331(c) no longer includes the introductory clause, "[n]otwithstanding the general rules in paragraphs (a) and (b) of this section."

Responses to comments regarding the exceptions in § 1033.221 are discussed in part IV.B.4. Regarding commenters' concern that small data providers would be overburdened by what they interpreted as a requirement under proposed § 1033.331(c) to track all authorizations and data access requests of their customers, § 1033.331(c) does not require recordkeeping. With

respect to concerns regarding the burden of policies and procedures requirements in § 1033.351(b) and (d) regarding responses to denials and record retention, the CFPB believes these requirements will not overburden data provider, as discussed more fully below in part IV.C.7 below. Additionally, as discussed in part IV.A.4, the final rule does not cover small depository institution data providers.

Jointly held accounts (§ 1033.331(d))

CFPA section 1033(a) generally requires data providers to make available "to a consumer, upon request, information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained." The statute does not directly address how this obligation applies with respect to jointly held accounts. The CFPB proposed in § 1033.331(d) to require a data provider that receives a request for covered data from a consumer that jointly holds an account or from an authorized third party acting on behalf of such a consumer to make available covered data to that consumer or authorized third party, subject to the other requirements of § 1033.331. The CFPB noted that this provision would not affect data providers' existing obligations to provide information directly to consumers under other Federal consumer financial laws, such as EFTA, TISA, and TILA, and their implementing regulations. Those regulations generally permit data providers to satisfy the relevant information disclosure requirements by providing the information to any one of the consumers on the account.[78] The CFPB requested comment on whether other account holders should receive authorization disclosures or otherwise be notified, or should have an opportunity to object, when an account holder authorizes access to consumer information. The CFPB also requested

[78] *See* 12 CFR 1005.4(c), 1030.3(d), 1026.5(d).

comment on whether the rule should specifically address whether authorized users of credit cards should have similar access, even if they are not a joint holder of the credit card account.

A nondepository commenter requested that the CFPB clarify that authorization from a single account holder is sufficient and that there is no requirement to notify other account holders. The commenter stated that this approach is consistent with other activity by an account holder, such as writing a check or accessing the account through a consumer interface, and that providing other account holders with notice and an opportunity to object would create legal questions and consumer friction for data access. A trade association for nondepository entities recommended that other account holders not be required to approve when an account holder authorizes access but that they should be notified and receive authorization disclosures. Another trade association for nondepository entities stated that the rule should require all account holders to provide authorization for access to covered data. The commenter stated that if the rule does not require authorization from all account holders, the other account holders should be notified and have an opportunity to object and prevent the authorization. A consumer advocate commenter stated that other account holders should not have the right to object but that they should receive notice unless the consumer authorizing access actively indicates that such notice would be harmful because it poses a risk to their safety.

For the reasons discussed herein, the CFPB is adopting § 1033.331(d) as proposed with one minor change. As finalized, § 1033.331(d) provides that a data provider that receives a request for covered data from a consumer that jointly holds an account or from an authorized third party acting on behalf of such a consumer must make available covered data to that consumer or authorized third party, subject to the other provisions of § 1033.331. The final rule changes "requirements" to "provisions" in the last phrase in § 1033.331(d) because the other

parts of the rule that identify circumstances in which a data provider may not be obligated to make available covered data are more accurately described as "provisions" than "requirements." Section 1033.331(d) carries out the objectives of CFPA section 1033(a) by clarifying whether a data provider must make available covered data in response to a request by one consumer with respect to covered data concerning a jointly held account.

Allowing a single account holder to request covered data or to authorize a third party to access covered data on behalf of the account holders is consistent with the broad authority that joint account owners have over the account. Given that broad authority, the CFPB concludes it would be unnecessarily burdensome at this time to require that other account holders approve in advance a request for covered data or authorize a third party to access covered data on behalf of a joint account holder. Likewise, the data provider or authorized third party is not required to provide notice or a copy of the authorization disclosure to other account holders. While a notice or authorization disclosure would inform the other account holders that account information is being accessed, the benefits of such a disclosure or notice are unclear and would depend on the circumstances, including the terms of the account and the relationship of the account holders. Each joint account holder already has significant authority over the account, including the ability to provide account information or expend funds. Moreover, when a joint account holder authorizes a third party to access covered data, the consumer protections in § 1033.421, including the limitations on collection, retention and use by authorized third parties, impose boundaries on the data that can be accessed by third parties and how that data can be used. Accordingly, the data provider is not required to provide a notice or copy of the disclosure to all joint account holders, though nothing in the rule prohibits data providers from doing so if they see fit.

Data provider revocation (§ 1033.331(e))

Proposed rule

The CFPB proposed in § 1033.331(e) to permit a data provider to make available to the consumer a reasonable method by which the consumer could revoke any third party's authorization to access all of the consumer's covered data. Under the proposed rule, to be reasonable, the revocation method would need to be, at a minimum, unlikely to interfere with, prevent, or materially discourage consumers' access to or use of the data, including access to and use of the data by an authorized third party. Indicia that the data provider's revocation method was reasonable would include its conformance to a qualified industry standard. Finally, under the proposed rule, a data provider that received a revocation request from consumers through a revocation method would be required to notify the authorized third party of the request.

The proposal stated that this provision, along with the proposed third party revocation requirements in § 1033.421(h), were intended to ensure consumers would have multiple outlets through which they could revoke third party authorization to access covered data. But the CFPB preliminarily determined that requiring data providers to make a revocation method available might burden smaller entities. The proposed rule also noted that stakeholders had expressed concerns during SBREFA about anticompetitive behaviors from data providers. Accordingly, the proposed rule would not have permitted data providers to make available a method through which the consumer could partially revoke a third party's access to covered data, as this would be inconsistent with proposed § 1033.201(a), requiring data providers to make covered data available upon request based on the terms of the consumer's authorization. The proposed rule stated that partial revocations could result in consumers losing utility of data access for certain use cases. To further account for anticompetitive concerns, proposed § 1033.331(e) included a

list of non-exhaustive requirements to ensure the optional revocation method would be reasonable, which were drawn from the definition of "information blocking" in section 3022(a) of the Public Health Service Act. The proposed rule stated that this language would promote consumers' ability to access and share their data by ensuring data providers do not impose obstacles that effectively evade their obligations to make available covered data under CFPA section 1033. Regarding the proposed notification requirement, the proposed rule explained that a third party whose authorization to access data is revoked by a consumer would need to understand that the consumer has chosen to end their authorization, and that the data provider did not terminate the access for another reason.

Comments received

The concept of revocation, including permitting data providers to provide consumers with a revocation method, received general support from commenters, with many agreeing that consumers benefit significantly from multiple opportunities to revoke third party authorizations. Some commenters, including a consumer advocate, a trade association for banks, and a third party commenter, stated that the CFPB should require, rather than permit, revocation through a data provider. A trade association for data providers stated that requiring revocation through data providers would not be a burden for smaller entities because core processors can supply interfaces that include revocation methods.

Some banks and consumer advocates expressed concerns about qualified industry standards related to revocation, stating that qualified industry standards are inappropriate for revocation and could conflict with federally supervised entities' regulatory obligations. Additionally, some data provider, third party, and data aggregator commenters expressed concern about the proposed notification requirement, and suggested the following changes:

require notification in as close to real-time as possible; require data providers to provide 24-hour notice to the third party before terminating access in case of pending transactions or fraud attempts; require consumers to notify all parties of their revocation and free data providers from possible liability that results from revocation; and ensure data providers do not have to furnish notification to any third party but the authorized third party. Third party commenters suggested that without more guardrails around the notification requirement, or around data providers' ability to solicit revocations from consumers, the rule would not adequately account for the potential for anticompetitive activities from data providers. In contrast, a trade association for banks requested that the CFPB make clear that a reasonable revocation method would allow the data provider to provide clear disclosures about data access to their customers.

Commenters also provided feedback on whether the permitted revocation method should allow partial revocations. Some data providers and data provider trade associations stated that the final rule should allow for partial revocations through the data provider for the consumer's added control. They also stated that the proposed rule overstated concerns about consumers not realizing the impacts of revocation on data access, commenting that consumers making post-authorization decisions to revoke reflect intention to control and terminate third party authorizations. Other data provider and credit union trade association commenters stated that partial revocation is costly and burdensome and could result in unfair competition.

A trade association for third parties and other stakeholders raised concerns about consumer revocation through the data provider in relation to TANs. Several third parties stated that consumer revocation could result in the consumer, intentionally or unintentionally, causing the data provider to revoke the consumer's TAN after the consumer obtains the third party product or service but before the payment settles. Commenters suggested that the proposed rule's

strict all-or-nothing revocation method for data providers could contribute to the unintended consequence of third party payment failure when a consumer had authorized a third party to access a TAN and other covered data.

Finally, commenters suggested that the CFPB: clarify that data providers must recognize revocation requests in joint accounts if one account holder makes the request; clarify the "all or nothing" requirement and how revocation works for joint account holders; clarify what constitutes a "reasonable method" and provide examples of when revocation mechanisms are likely to interfere with, prevent, or materially discourage consumers and how deceptive design might manifest in revocation mechanisms.

Final rule

For the reasons discussed herein, the CFPB is finalizing § 1033.331(e) with certain changes and one technical correction described below, to provide that a data provider does not violate the general obligation in § 1033.201(a)(1) by making available to the consumer a reasonable method to revoke any third party's authorization to access all of the consumer's data, provided that such method does not violate § 1033.201(a)(2). Indicia that the data provider's revocation method is reasonable include its conformance to a consensus standard. A data provider that receives a revocation request from a consumer through a revocation method it makes available must revoke the authorized third party's access and notify the authorized third party of the request in a timely manner. Section 1033.331(e) carries out the objectives of CFPA section 1033(a) by clarifying that a data provider is permitted to establish certain procedures allowing a consumer to communicate efficiently and directly with the data provider when a third party is no longer authorized to act on the consumer's behalf to access covered data.

While consumers benefit from multiple methods of revoking third party authorization to access covered data, the CFPB has determined that requiring data providers to make available a revocation method would not be necessary and could be burdensome for some data providers. The CFPB expects that consumers seeking to revoke access to a requested product or service are most likely to do so from the third party with whom they have the ongoing customer relationship. As discussed above, while one commenter stated that requiring revocation through data providers would not be burdensome because entities could request core processors to include a method as part of their consumer interfaces, other commenters raised concerns about the burdens associated with maintaining an optional revocation method that adheres to the rule's requirements. Though providing a revocation method itself could be relatively straightforward, the CFPB acknowledges commenters' concerns that ongoing costs associated with maintaining it could be burdensome. As such, the final rule permits, but does not require, data providers to provide a revocation method to consumers.

The proposed rule stated that, to be reasonable, the revocation method would, at a minimum, need to be unlikely to interfere with, prevent, or materially discourage consumers' access to or use of the data, including access to and use of the data by an authorized third party. This language was intended to ensure data providers offering an optional revocation method did not impose obstacles that evade their obligations to make available covered data under CFPA section 1033. The final rule instead states that data providers do not violate their general obligation in the rule by making available to the consumer a reasonable method to revoke any third party's authorization to access all of the consumer's covered data, provided that such method does not violate § 1033.201(a)(2). This change is meant to ensure that any revocation method a data provider offers to consumers adheres to the prohibition against evasion, which

applies to all other data provider activities, and is meant to achieve the same effect behind the proposed rule's language: data providers must not violate their general obligation to make available covered data through the offering of the optional revocation method. Potential examples of actions that might violate the prohibition against evasion in providing an optional method for consumers to revoke third party authorizations are intentionally soliciting consumers to revoke authorizations based on misleading statements about the third parties' collection, use, or retention of covered data, or providing granular revocations or disabling a TAN without the consumer's consent, discussed further below.

As discussed above, some commenters were concerned that consensus standards could be inappropriate for revocation and could conflict with federally supervised entities' regulatory obligations. The CFPB notes that consensus standards are indicia of compliance, not mandatory for compliance, and the revocation method itself is optional. Without suggesting that any such conflict exists, the CFPB is accordingly confident that data providers can avoid any hypothesized conflict with other obligations.

The CFPB remains concerned that data providers are likely to have commercial interests contrary to those of authorized third parties offering competing products or services. As such, the final rule requires data providers that provide consumers a revocation method to make available a method through which the consumer can revoke access to all of the consumer's covered data, adhere to the final rule's anti-evasion provision in § 1033.201(a)(2) and notify the authorized third party of the request in a timely manner. This language will ensure that any revocation method provided to consumers is provided in accordance with the anti-evasion provision in § 1033.201(a)(2).

While some commenters argued that data providers should be allowed to provide consumers the option to request partial revocations through the data provider, the final rule only allows for all-or-nothing revocations. Commenters did not describe in detail data providers' view into the functionality of products or services, and therefore it remains unclear how a data provider could effectively determine how to provide partial revocations that do not result in harms to consumers or authorized third parties as they continue to access covered data for products and services for which the authorization is intended to remain in place. As discussed above regarding data providers responding to requests under § 1033.331(b)(1), some data provider commenters expressed concern that data providers were not positioned to have actual knowledge of third parties' receipt of authorization from consumers. The CFPB has determined that, just as data providers are not in the best position to manage third party authorizations, data providers are likewise not in the best position to allow consumers to seek partial revocations, a consequence of which would be termination of third parties' access to potentially reasonably necessary data elements. Further, data providers' incentives to provide partial revocations are unclear, and may not be aligned with consumers' incentives to control the authorizations they provide to third parties in order to receive products or services. As discussed above regarding data providers responding to requests under § 1033.331(b)(1), data providers may have strong incentives to limit the scope of data available to third parties, especially those providing a competing product or service. These potentially competing incentives may result in competition harms or consumer harms if data providers are permitted to provide consumers with the ability to only partially revoke third party authorizations to access covered data.

Additionally, as described above, some commenters suggested that the proposal's all-or-nothing revocation method for data providers could contribute to the unintended consequence of

third party payment failure when a consumer had authorized a third party to access a TAN and other covered data and the consumer subsequently requests revocation of that information. Commenters expressed concern that a consumer's revocation of TAN information would also result in a data provider disabling a TAN's functionality. However, there are multiple reasons a consumer might revoke a third party's access to TAN information. A consumer may revoke access to the TAN information because they do in fact want to stop a third party's ability to initiate payments—therefore, the revocation would be intended for both the information and the functionality. Sometimes the consumer may just intend to revoke the third party's ability to access information, but intend for the TAN to remain functional. To avoid violating the anti-evasion provision in § 1033.201(a)(2), data providers must be aware that disabling a TAN without the consumer's consent might render unusable the covered data that the data provider makes available or prevent, interfere with, or materially discourage a consumer in accessing covered data. Whether revocation of TAN information or TAN functionality following a consumer's revocation request is a material interference with the third party's access to covered data will depend on the facts. However, general awareness of the possibility of unintended consequences of revocation, without more, will not be enough to violate this standard.

Further, the CFPB agrees with commenters that § 1033.331(e) should specify that revocation must occur in a timely manner and thus has included language to that effect in the final rule. Failure to timely revoke data access is likely to interfere with a consumer's express desire to revoke a third party's authority to access covered data. Similarly, failure to notify third parties of consumers' revocation requests in a timely manner could result in the third party continuing to seek access to covered data and receiving denials to those requests. As such, to ensure revocation is timely following a revocation request, and that notification is provided to

the authorized third party in a timely manner, the final rule requires that: (1) the third party's access to the data must be revoked in a timely manner; and (2) a data provider that receives a revocation request from a consumer through a revocation method it makes available must notify the authorized third party of the request in a timely manner. While commenters suggested other specific changes to the notification requirements, described above, the CFPB has determined that additional changes are unnecessary.

Finally, a data provider commenter and trade associations for banks asked that the final rule provide information about how revocation works for joint account holders. As discussed related to § 1033.331(d), a consumer that jointly holds an account may request access to covered data or may authorize third party access to covered data. Likewise, the revocation method described in § 1033.331(e) pertains to a consumer that jointly holds an account. Any consumer that jointly holds an account may revoke third party authorization to access covered data related to that account, if provided for under the terms of the account. The CFPB has made a technical correction to the last sentence in proposed § 1033.331(e) to refer to revocation requests received from "a consumer," instead of the plural "consumers," which could have otherwise implied both joint account holders always need to provide the revocation request.

6. Public disclosure requirements (§ 1033.341)

Public disclosure and human- and machine-readability requirements (§ 1033.341(a))

Proposed § 1033.341(a) would have required data providers to make the information described in proposed § 1033.341(b) through (d)—which address identifying information about the data provider, developer interface documentation, and performance specification—readily identifiable to members of the public. Proposed § 1033.341(a)(1) defined this to mean that the information must be at least as available as it would be on a public website. Under proposed

§ 1033.341(a)(2), the information would have been required to be available in both human- and machine-readable formats. The CFPB preliminarily determined that making the data available in a machine-readable format could enable third parties and other stakeholders to use automated processes to ingest the relevant information into their systems for processing and review, which will make the process of obtaining this information more efficient. The CFPB requested comment on whether it should indicate that conformance to a specific standard or a qualified industry standard would be relevant indicia for a data provider's compliance with the machine-readability requirement in proposed § 1033.341(a)(2). Additionally, the CFPB requested comment on whether it should issue rules or guidance that would make it easier for third parties and other members of the public to identify a particular data provider's information.

Commenters generally supported the requirement to make information about the data provider readily identifiable. Some commenters recommended the rule go further regarding public disclosure requirements. One bank commenter recommended that the rule allow for multiple data providers to publish their required disclosures in one location. The commenter suggested that this may be more efficient for data providers and might reduce search costs for members of the public seeking to access disclosures from multiple data providers. Further, one standard-setting organization commenter suggested that an already-existing registry where data providers self-report data to help third parties connect to their data might also function as a repository for disclosures of developer interface documentation.

Regarding the proposed requirement to make information available in both human-readable and machine-readable formats, a research institute and a trade association suggested that data provider disclosures should meet the proposed machine-readability requirement if a data provider makes the information available in a format that consumers can print or retain. In

response to the request for comment, one industry commenter recommended that the CFPB should either provide a standard for machine-readability or make conformance with a consensus standard indicia of compliance.

For the reasons discussed herein, the CFPB is finalizing § 1033.341(a) as proposed. The CFPB agrees with the commenters that a central repository could benefit the public by reducing search costs. A data provider could comply with § 1033.341(a) by publishing on its website a link, readily identifiable to members of the public, that redirects consumers to the disclosures required in § 1033.341(b) through (d), published on a publicly available central repository, provided the data provider does not otherwise impede the public's ability to readily locate the disclosures.

In response to comments, information that is only available in a human-readable format that a consumer can print or retain, but that is not also available in a machine-readable format, would not comply with § 1033.341(a). As explained in the proposal, making the data available in a machine-readable format enables third parties and other stakeholders to use automated processes to ingest the relevant information into their systems for processing and review, which will make the process of obtaining this information more efficient.

Final § 1033.341(a), as well as final § 1033.341(b) through (c), will carry out the objectives of CFPA section 1033 by ensuring that third parties can efficiently access information necessary to make requests for covered data and use a developer interface. By enabling third parties to obtain information about how to use the developer interface, § 1033.341(a) through (c) also promotes the use and development of standardized formats available through the developer interface.

Disclosure of identity information and contact information (§ 1033.341(b))

The CFPB proposed in § 1033.341(b) to require data providers to disclose certain identifying information in the manner described in proposed § 1033.341(a). Specifically, proposed § 1033.341(b)(1) through (3) would require data providers to publicly disclose certain identifying information: their legal name and, if applicable, any assumed name they are using when doing business with the consumer; a link to their website; and an LEI issued by a utility endorsed by the LEI Regulatory Oversight Committee or a utility endorsed or otherwise governed by the Global LEI Foundation (or any successor thereof) after the Global LEI Foundation assumes operational governance of the global LEI system. Proposed § 1033.341(b)(4) would have required data providers to disclose contact information that enables a consumer or third party to receive answers to questions about accessing covered data under part 1033.

Commenters provided little feedback about proposed § 1033.341(b). One LEI nondepository entity commenter supported the requirement for data providers to disclose their LEI, noting that consistent use of these identifiers will enable a more efficient data sharing process. Two credit union trade association commenters suggested that smaller data providers that use a separate vendor to maintain their developer interface should be able to provide that vendor's contact information for inquiries related to the interface.

For the reasons discussed herein, the CFPB is finalizing § 1033.341(b) as proposed. A data provider is permitted to provide the contact information for the vendor that maintains the developer interface for inquiries related to the developer interface. The rule does not require that a data provider itself respond to inquiries related to its developer interface. The rule does not require that a data provider itself respond to such inquiries. Rather, it requires that data providers

provide contact information that enables a consumer or third party to receive answers to questions about accessing covered data, which reasonably allows a data provider to direct such inquiries to a vendor that develops and maintains the interface.

Disclosure of developer interface documentation and access location (§ 1033.341(c))

The CFPB proposed to require in § 1033.341(c) that a data provider disclose for its developer interface, in the manner described in proposed § 1033.341(a), documentation, including metadata describing all covered data and their corresponding data fields, and other documentation sufficient for a third party to access and use the interface. Under proposed § 1033.341(c), a data provider would need to maintain and update documentation as the developer interface is updated. The CFPB also proposed that the documentation include information on how third parties can get technical support and report issues with the interface. Finally, the CFPB generally proposed to require that developer interface documentation must be easy to understand and use. The CFPB preliminarily determined that it is common practice for data providers that have interfaces to disclose such metadata and documentation. Additionally, the CFPB preliminarily determined that a requirement to publicly disclose documentation and metadata would not materially increase the cost of compliance and would substantially enhance the usability of the interface.

One commenter that provides services to data providers highlighted generally the types of challenges industry participants might have in accessing data from a data provider. The commenter did not identify any particular challenges stemming from the proposal but emphasized the importance of industry alignment on the type of information needed to access and use APIs effectively. The commenter focused on the challenges of accessing and using a

production API when its specifications are not publicly available and regularly maintained.[79] Another industry commenter supported the proposed requirement that data providers disclose information sufficient for a third party to access and use the interface.

However, several data provider commenters and a research institute commenter were critical of the proposed requirement that data providers disclose developer interface documentation and metadata sufficient for a third party to access and use the interface. These commenters stated that it is not common practice for data providers to make developer interface metadata and documentation available to the public and would subject data providers to security risks. These commenters recommended that the information required to be disclosed publicly should not be sufficient, on its own, for a third party to access and use the interface.

A bank commenter, research institute commenter, and bank trade association commenter opposed the requirement in proposed § 1033.341(c)(1) to update documentation as the developer interface is updated. These commenters explained that this requirement would be unduly burdensome to data providers. These commenters noted that a developer interface typically requires frequent, minor changes that do not significantly affect access or use, and the proposed requirement would be costly to implement. These commenters suggested instead that data providers be required to reasonably cooperate with authorized third parties to make available documentation in a timely manner that enables the connectivity requirements provided in part 1033.

For the reasons discussed herein, the CFPB is finalizing § 1033.341(c) with certain revisions to address commenters' concerns about the information security risks and burden.

[79] *See, e.g.*, Dr. Paul M. Cray, *Open API Specifications in the Real World*, at 5-15 (APIContext, White Paper, Aug. 2024), https://www.regulations.gov/comment/CFPB-2023-0052-11139 (noting, generally, that public disclosure of performance specifications poses some challenges for data providers, but overall is the correct approach for industry).

Specifically, final § 1033.341(c) requires a data provider to disclose in the manner required by § 1033.341(a) documentation about its developer interface, including metadata describing all covered data and their corresponding data fields, and other documentation sufficient for a third party to access and use the interface. Final § 1033.341(c) provides that a data provider is not required to make publicly available information that would impede the data provider's ability to deny a third party access to its developer interface, consistent with § 1033.321. Indicia that documentation is sufficient for a third party to access and use a developer interface include conformance to a consensus standard.

Final § 1033.341(c) also provides that the documentation must be maintained and updated as reasonably necessary for third parties to access and use the interface in accordance with the terms to which data providers are subject under part 1033. Further, the documentation must include how third parties can get technical support and report issues with the interface. In addition, the documentation must be easy to understand and use, similar to data providers' documentation for other commercially available products. Publishing information about how third parties can access and use the developer interface, including metadata describing all covered data and their corresponding data fields, will promote the development and use of standardized formats of information, consistent with CFPA section 1033(d).

In proposing § 1033.341(c), the CFPB did not intend for data providers to make publicly available access keys to the developer interface or other information that would undermine the purpose of § 1033.321. To address commenters' concerns that the proposal might interfere with their ability to engage in appropriate risk management, the final rule clarifies that a data provider is not required to make publicly available information that would impede its ability to reasonably deny a third party access to its developer interface, consistent with § 1033.321. The final rule's

inclusion of a consensus standard as indicia for what documentation is sufficient to access and use a developer interface is intended to promote standardization with respect to the type of documentation that facilitates third parties' access to and use of covered data, while accounting for information security risks to data providers.

The proposal would have required documentation to be updated "as the developer interface is updated." To address concerns regarding the potential burden of documenting frequent minor updates to developer interfaces, final § 1033.341(c)(1) provides that such documentation must be maintained and updated "as reasonably necessary for third parties to access and use the interface in accordance with the terms to which data providers are subject" under part 1033. This change from the proposal provides flexibility for data providers to make minor updates to their interfaces without requiring an update to the corresponding documentation, as long as third parties can still access and use the interface as required by the final rule.

The CFPB declines to adopt commenters' recommendation to require data providers to cooperate with third parties to make documentation available in a timely manner. The CFPB is concerned this could imply that third parties engage in some affirmative conduct to obtain updated documentation, which could undermine the rule's affirmative requirement to make the information publicly available, which could create inefficiencies for many third parties. Further, the CFPB does not believe this change is necessary in light of revisions to § 1033.341(c)(1).

Performance disclosure (§ 1033.341(d))

Proposed § 1033.341(d) would have required that a data provider disclose, in the manner described in proposed § 1033.341(a), information about the performance of its developer interface for each month. Specifically, the CFPB proposed that on or before the 10th calendar

day of each month, the data provider would disclose the quantitative minimum performance specification in proposed § 1033.311(c)(1)(i) achieved in the previous calendar month. The CFPB proposed to require that the data provider's disclosure include at least a rolling 13 months of the required monthly figure, except that the disclosure need not include the monthly figure for months prior to the compliance date applicable to the data provider. The CFPB proposed to require that the data provider disclose the metric as a percentage rounded to four decimal places, such as "99.9999 percent."

The CFPB requested comment on whether the final rule should require data providers to disclose additional performance metrics, including those required to be disclosed in other jurisdictions' open banking systems, such as the volume of requests, the number of accounts and/or consumers with active authorizations, uptime, planned and unplanned downtime, and response time.

One data aggregator commenter recommended that a final rule include additional performance metrics. Specifically, this commenter suggested the disclosures include information about when access caps were put in place and how long they lasted, uptime, latency, days of planned and unplanned downtime, and days of notice for unplanned downtime. This commenter stated that disclosure of these metrics would help the CFPB determine whether consumers benefit from their data access rights and identify areas where further guidance or action is advisable. Finally, this commenter stated that these additional metrics would help third parties determine if they were being treated in a discriminatory manner compared to other third parties.

A bank commenter, a research institute commenter, and a bank trade association commenter stated that ten calendar days after the end of a month is not enough time to publish performance data for that month on the grounds that more time is necessary for the data provider

to ensure the accuracy of the data being transmitted. These commenters stated that it can take more than a week for data providers' internal databases to populate the required information for the performance metrics. These commenters suggested that the period for data providers to disclose performance statistics should be 45 days or, at a minimum, ten business days after the close of the month. A data provider trade association also recommended that data providers be able to make these disclosures on a quarterly basis. By contrast, a data aggregator commenter suggested that performance data should be available in real time and on demand on the grounds that real-time availability would help data providers discover and address security vulnerabilities in their developer interfaces.

A bank trade association commenter suggested that the CFPB use more precise language in § 1033.341(d) as to which disclosures are intended to be visible to the public, as opposed to disclosures that should be available only for third parties seeking access to the developer interface. A bank research institute commenter and a bank trade association commenter stated that the final rule should allow for multiple data providers to publish their disclosures of developer interface performance data in one location. These commenters suggested that a single location may be more cost-effective for data providers and might reduce search costs for members of the public seeking to access disclosures from multiple data providers. Additionally, these commenters recommended that the CFPB clarify that data providers would meet the requirements to make performance metrics readily identifiable to the public if multiple data providers published their metrics in one location. A bank trade association commenter stated that the proposed requirement to disclose performance metrics would not result in any consumer benefit. This commenter further stated that such a requirement would increase costs for data

providers but that consumers cannot benefit from knowledge of metrics about a process in which consumers do not directly participate.

For the reasons discussed herein, the CFPB is finalizing the requirement in § 1033.341(d), with minor modifications. Publicly available performance data will inform consumers and authorized third parties about whether a data provider is maintaining commercially reasonable performance, which will promote data provider accountability. Contrary to some commenters' belief, performance metrics will also help consumers who struggle to connect a third party mobile banking application to their account with a data provider to understand the source of the issue. As an additional benefit, consistent with the CFPA's objective under section 1021 that markets for consumer financial products and services operate transparently and efficiently to facilitate access and innovation, availability of performance metrics should also help consumers select a data provider by allowing them to shop and select a data provider based on their developer interface performance.

Final § 1033.341(d) requires a data provider to disclose, on or before the final day of each calendar month, in the manner required by § 1033.341(a), the quantitative minimum performance specification for the response rate described in § 1033.311(c)(1)(i) through (iv) that the data provider's developer interface achieved in the previous calendar month. The data provider's disclosure must include at least a rolling 13 months of the required monthly figure, except that the disclosure need not include the monthly figure for months prior to the compliance date applicable to the data provider. The data provider must disclose the metric as a percentage rounded to four decimal places, such as "99.9999 percent." The final rule also modifies the title of § 1033.341(d) to "Performance disclosure" to more accurately reflect the requirement.

Final § 1033.341(d) does not require disclosure of developer interface performance metrics other than proper response, as defined in final § 1033.311(c)(1)(i) through (iv). Regarding a commenter's request that the CFPB require disclosure of additional performance metrics, the CFPB notes that it did not propose specific definitions for latency, uptime, or downtime, nor did the commenter provide definitions. The CFPB believes such metrics would benefit from further analysis to ensure disclosures are made consistently to enable meaningful comparisons and analysis of commercially reasonable performance. The CFPB likewise declines to add disclosures about data access caps to the final § 1033.341(d). Data access caps must be reasonable under final § 1033.311(d), but this requirement is not part of the quantitative minimum performance specification of § 1033.311(c). Access caps may vary based on a number of factors, including the threshold metric, the type of request, and the period of time they are in place The proposal did not define how an access cap (or caps) could be disclosed and the CFPB is concerned such a disclosure would be complex and disclosed inconsistently, and thus would not provide meaningful information to the public.

To address commenters' concerns regarding the timing for disclosures, final § 1033.341(d) provides that data providers must make their disclosures by the final day of each calendar month, rather than by the tenth calendar day as proposed. Requiring disclosure by the end of the next month should give data providers a reasonable amount of time to run and audit the required reports to calculate the quantitative minimum performance specification, as this is longer than the ten business days some commenters suggested as the minimum time needed to perform these analyses. A full month to disclose the required performance metrics should promote quality control of the data and will ensure that the information will be made publicly available on a predictable basis. Requiring data providers make these disclosures less frequently,

such as on a quarterly basis, would reduce the incentive for data providers to remedy performance deficiencies in a timely manner.

Requiring real-time reporting of the quantitative minimum performance specification as suggested by one commenter, however, is unlikely to assist in the identification of security vulnerabilities. This metric merely tracks the rate at which the developer interface gives proper responses to requests and would likely provide little insight into whether an update to the interface had introduced a security vulnerability. The CFPB is thus not adopting a real-time reporting requirement.

Final § 1033.341(d) carries out the objectives of CFPA section1033(a).[80] Publicly available performance data are relevant for consumers and authorized third parties seeking reliable access to consumer-authorized data. As an additional benefit, consistent with the CFPA's objective under section 1021 that markets for consumer financial products and services operate transparently and efficiently to facilitate access and innovation, availability of performance metrics should also help consumers select a data provider by allowing them to shop and select a data provider based on their developer interface performance.

7. Policies and procedures (§ 1033.351)

Reasonable written policies and procedures (§ 1033.351(a))

The CFPB proposed in § 1033.351(a) to set forth a general obligation that data providers establish and maintain written policies and procedures that are reasonably designed to achieve the objectives set forth in proposed subparts B and C of the rule, including proposed § 1033.351(b) through (d). Under the proposal, a data provider would need to periodically

[80] The proposal preliminarily relied on section 1032 of the CFPA, but it is not necessary to rely on that authority in this final rule.

review the policies and procedures required by proposed § 1033.351 and update them as appropriate to ensure their continued effectiveness. The CFPB explained that, to minimize impacts on data providers, including avoiding conflicts with any overlapping compliance obligations, proposed § 1033.351(a) required data providers to tailor these policies and procedures to the size, nature, and complexity of their activities.

Commenters including banks, third parties, and consumer advocacy groups, generally supported the proposed requirements for data provider policies and procedures. One data provider industry commenter specifically supported the statement that data provider policies and procedures be appropriate to the size, nature, and complexity of the data provider's activities. Some commenters recommended revisions to specific policies and procedures provisions or challenged the CFPB's authority to issue a particular policies and procedures requirement. These comments are discussed in more detail in this section below.

For the reasons discussed herein, the CFPB is finalizing § 1033.351(a) generally as proposed, with one clarification. Under the final rule, as proposed, a data provider must establish and maintain written policies and procedures that are reasonably designed to achieve the objectives set forth in subparts B and C of the final rule. Policies and procedures must be appropriate to the size, nature, and complexity of the data provider's activities. Further, as proposed, a data provider must periodically review the policies and procedures required by this section and update them as appropriate to ensure their continued effectiveness.

In light of comments, the final rule includes new language stating that a data provider has flexibility to design policies and procedures to avoid acting inconsistently with its other legal obligations or in a way that could reasonably hinder enforcement against unlawful or potentially

unlawful conduct. This revision is discussed in more detail in the discussion of § 1033.351(b)(2), below.

Policies and procedures for making covered data available and responding to requests (§ 1033.351(b))

Making covered data available (§ 1033.351(b)(1))

Proposed § 1033.351(b) would have required data providers to establish policies and procedures reasonably designed to make covered data available. Proposed § 1033.351(b)(1) would have required that the policies and procedures required by proposed § 1033.351(a) are reasonably designed to ensure that data providers create a record of the data fields that are covered data in the data provider's control or possession, what covered data are not made available through a consumer or developer interface pursuant to an exception in § 1033.221, and the reasons the exception applies. The CFPB explained that documentation of the fields that are made available in accordance with the covered data definition could help the CFPB identify compliance gaps in what the data provider makes available, streamline negotiations between data providers and third parties by establishing the available data fields, and encourage the market to adopt more consistent data sharing practices.

Under the proposal, a data provider would have been permitted to comply with the proposed § 1033.351(b)(1) requirement by incorporating the data fields defined by a qualified industry standard, provided doing so is appropriate to the size, nature, and complexity of the data provider's activities. However, exclusive reliance on data fields defined by such a standard would not be appropriate if such data fields failed to identify all the covered data in the data provider's control or possession. The CFPB preliminarily concluded that allowing a data provider to cite data fields defined by a qualified industry standard, to the extent that standard

identifies covered data in the data provider's control or possession, could ease the compliance burden on data providers and promote market standardization according to CFPA section 1033(d). The CFPB proposed these requirements to facilitate compliance with and enforcement of the general obligation in proposed § 1033.201.

The CFPB received some support for the provisions in proposed § 1033.351(b)(1). One Member of Congress supported this requirement, stating that it would help ensure that consumer data are not withheld for anticompetitive reasons. Some data provider commenters expressed concern that the provision's reference to qualified industry standards would be of little utility to data providers, on the grounds that data providers would not be able to rely on the qualified industry standard to demonstrate compliance because such standard likely would not define all the data in the control or possession of the data provider. One data provider trade association stated that neither the statutory text nor the congressional intent of CFPA section 1033 calls for data providers to create and maintain the enumerated records. This commenter suggested that data providers already have supervisory obligations and that the CFPB does not have the authority for streamlining the negotiations of private commercial actors.

For the reasons discussed herein, the CFPB is finalizing § 1033.351(b)(1) with modifications to further clarify what data fields are required to be made available. Final § 1033.351(b)(1) states that indicia that a data provider's record of applicable data fields complies with the requirements of § 1033.351(b)(1) include listing data fields that conform to those published by a consensus standard. The final rule does not include the proposed regulatory text that would have stipulated that exclusive reliance on data fields defined by a qualified industry standard would not be appropriate if such data fields failed to identify all the covered data in the data provider's control or possession. This change conforms § 1033.351(b)(1) to other

parts of the rule that utilize consensus standards as indicia of compliance. Additionally, the indicia approach addresses commenters' concerns that such standards may not reflect all of the data in control or possession of a data provider, while signaling to data providers that they may have additional data fields beyond the consensus standard that must be disclosed under the rule. For example, some of the terms and condition examples in § 1033.211(d) might be data fields that are not included in a consensus standard but would still be required under § 1033.351(b)(1).[81]

The CFPB is finalizing the other provisions in § 1033.351(b)(1) largely as proposed. As such, under § 1033.351(b)(1) a data provider is required to maintain policies and procedures reasonably designed to ensure that the data provider creates a record of the data fields of covered data in the data provider's control or possession. Section 1033.351(b)(1) also requires a data provider to record what covered data are not made available through a consumer or developer interface pursuant to an exception in § 1033.221, and the reason(s) the exception applies.

The CFPB is finalizing § 1033.351(b)(1) pursuant to its authority provided by CFPA sections 1033(a) and 1022(b)(1). The policies and procedures in § 1033.351(b) will carry out the objectives of CFPA section 1033(a) to make available information upon request by ensuring data providers are accountable for their decisions to make available covered data in response to requests, and in granting third parties access to the developer interface. Importantly, the policies and procedures required in § 1033.351(b)(1) are intended to ensure ongoing, consistent availability of the consumer's covered data fields. While data providers may be subject to supervisory requests for information related to their current data fields, as one commenter

[81] As discussed in part IV.A.6 (definition of consensus standard), as a general matter, the indicia of compliance framework maintains the final rule as the applicable legal standard while giving due weight to a fair, open, and inclusive consensus standard as evidence of compliance with the rule.

suggested, such a supervisory inquiry would likely occur after a consumer is harmed. Conversely, with proposed § 1033.351(b)(1), the consumer or the consumer's authorized third party have the opportunity to understand why covered data was not made available and potentially raise an issue with the data provider, or alternatively to adjust their own future requests for covered data to avoid repeated denials.

Efficiencies in onboarding third parties onto data providers' developer interfaces will enable the CFPB to administer and carry out the objectives of CFPA section 1033(a) to make available information upon request as well as the standardization objectives of CFPA section 1033(d). Creating a record of what data fields are covered data in the control or possession of the data provider will further the objectives of CFPA section 1033(a) and § 1033.211, by defining what constitutes "covered data" with respect to the data provider under the rule. Further, the record of data fields required under § 1033.351(b)(1) will ensure that data providers carry out their obligation to make "covered data" available, and that data providers do so in a consistent, objective manner, that can be reviewed and compared with data providers' actual practices by regulators in the course of supervisory and enforcement activities. This will ensure data providers are consistently making data available to all third parties and will reduce the costs of the onboarding process, which has been a problem in the past. This standardization is consistent with the objectives of CFPA section 1033(d).

Denials of requests for developer interface access and requests for information (§ 1033.351(b)(2) and (3))

Proposed § 1033.351(b)(2) would have required data providers to have policies and procedures that are reasonably designed to ensure that when a data provider denies a third party access to a developer interface pursuant to § 1033.321, the data provider: (1) creates a record

explaining the basis for denial; and (2) communicates to the third party, electronically or in writing, the reason(s) for the denial, and that the communication occurs as quickly as is practicable. Additionally, under proposed § 1033.351(b)(3) a data provider would have been required to reasonably design its policies and procedures to ensure that when it denies a request for information pursuant to § 1033.331, the data provider: (1) creates a record explaining the basis for denial; and (2) communicates to the consumer or the third party, electronically or in writing, the type(s) of information denied and the reason(s) for the denial, and that the communication occurs as quickly as is practicable. The CFPB requested comment on whether the final rule should provide examples or further clarify how data providers could reasonably design policies and procedures to account for data security or risk management concerns.

A third party commenter and a consumer advocacy group commenter recommended that the data provider be required to explain what actions or steps a consumer or third party must take to address a denial under proposed § 1033.351(b)(2) and (3). A bank trade association suggested that some third parties may be on a sanctions list[82] and asked the CFPB to clarify that the data provider does not need to engage with these third parties or inform them of the reason for the denial. Additionally, one bank commenter suggested that under proposed § 1033.351(b)(3) it would be difficult for a data provider to communicate to a consumer why a § 1033.331 denial occurred, on the grounds that this denial would typically happen before the data provider authenticated the consumer's identity. Finally, a bank trade association commenter suggested that the CFPB clarify that records explaining why a data provider denied a particular request do not need to include the data provider's specific risk management conclusions, on the grounds

[82] For example, a list released by the OFAC, such as the Specially Designated Nationals and Blocked Persons list.

that divulging specific risk management information could present additional security risks to the data provider.

For the reasons discussed herein, the CFPB is finalizing § 1033.351(b)(2) and (3) with certain revisions discussed below. Section 1033.351(b)(2) and (3) will carry out the objectives of CFPA section 1033 by enabling consumers and prospective authorized third parties to understand and satisfy data provider conditions necessary to make requests. Additionally, these provisions will prevent evasion by ensuring data providers do not avoid their obligations under CFPA section 1033 by denying developer interface access or information requests for unstated impermissible reasons.

Under final § 1033.351(b)(2) a data provider is required to reasonably design its policies and procedures to ensure that when the data provider denies a third party access to a developer interface pursuant to § 1033.321, the data provider: (1) creates a record substantiating the basis for denial; and (2) communicates in a timely manner to the third party, electronically or in writing, the reason(s) for the denial. Likewise, under final § 1033.351(b)(3), a data provider is required to reasonably design its policies and procedures to ensure that when the data provider denies a request for information pursuant to § 1033.331, to the extent the communication of the denial is not required to be standardized by § 1033.311(b), the data provider: (1) creates a record substantiating the basis for denial; and (2) communicates in a timely manner to the consumer or third party, electronically or in writing, the type(s) of information denied, if applicable, and the reason(s) for the denial.

The final rule revises the "as quickly as practicable" language from proposed § 1033.351(b)(2) and (3) to "in a timely manner" to conform to similar language about timeliness used in the regulation in the example to § 1033.331(b) and in § 1033.331(e), and is not intended

as a substantive change. For clarity, the final rule clarifies that the requirement for policies and procedures to be designed to communicate the reasons for denials applies to when a denial occurs for a reason described in § 1033.331(c), As discussed in part IV.C.5 above, § 1033.331(c) cross-references the provisions of the rule that allow a data provider to deny a request for information. Additionally, the final rule requires policies and procedures to provide information when information is denied pursuant to a consumer or third party request "if applicable." A request for information will not always be denied for reasons related to specific information requested. For example, a denial under § 1033.331 could occur due to the data provider not having sufficient information to authenticate or confirm authorization under § 1033.331(a) and (b), or because the interface is unavailable, and thus there would be no specific information to be specified in those cases.

Section 1033.351(b)(2) and (3) will provide data providers rule with appropriate flexibility to allow them to comply with other regulatory obligations, while still generally enabling consumers and third parties to understand reasons for denials in a timely manner and reduce the potential for pretextual denials. Without these policies and procedures requirements, compliance obligations with §§ 1033.321 and 1033.331 would be difficult to administer, ultimately harming the consumer as a result.

Revisions in § 1033.351(b)(3) are intended to distinguish denials from the standardized format requirement in § 1033.311(b). The text in § 1033.351(b)(3) retains the ability of the data provider to have flexible policies and procedures governing denials of information requests. These denials differ, somewhat, from § 1033.311(b) error codes, because the conditions of § 1033.331(b) are not intended to impose specific expectations as to how the data provider

considers these conditions, whereas § 1033.311(b) error codes have more prescriptive requirements, as discussed in this section below.

For purposes of § 1033.351(b)(3), a denial of an information request occurs when the data provider does not make data available pursuant to § 1033.331(c). Such a denial might be communicated pursuant to standardized communication protocols under § 1033.311(b), such as through an error code. These communication protocols might also include communications of other responses that are not denials but are relevant to fulfilling the request. For example, when an authorized third party requests a nonexistent data field, under § 1033.311(b) a standardized response is required to be given to the requestor, informing them of the deficient request. Conversely, under a § 1033.351(b)(3) denial, a data provider is informing the requestor that they are not being granted access to particular information in the developer interface pursuant to § 1033.331. After this communication, the data provider's obligations to the consumer or third party are satisfied, save for the records to be retained under § 1033.351(d). Under § 1033.351(d)(2)(i) and (ii), discussed below, a data provider must establish and maintain policies and procedures to retain records of, among other things, requests for a third party's access to an interface and records of requests for information. Additionally, under final § 1033.351(d)(2)(v), a data provider must establish and maintain policies and procedures to retain records of § 1033.311(c)(2) commercially reasonable performance specifications. Accordingly, records of both standardized error code denials pursuant to § 1033.311(c)(2) and denials of information requests under § 1033.351(b)(3) must be retained.

For clarity, final § 1033.351(b)(2)(i) and (3)(i) uses "substantiating" in place of "explaining." The proposed rule used the terms interchangeably. The use of "substantiate" in the final rule clarifies that associated evidence for the denial should be retained as part of the data

provider's required policies and procedures. Additionally, this change will not create a substantial documentation burden for data providers, given that these records are already being kept. Including a requirement for data providers to explain the process for the consumer or third party to remedy a reason for denial, as suggested by some commenters, would be an unnecessary addition to the final rule. The CFPB did not propose these appeal processes, and, if there were a denial under § 1033.351(b)(3), the process would be for the consumer or third party to again request access to the covered data after correcting the deficiency explained under § 1033.351(b)(3)(ii). If the data provider denied a valid request, then the data provider would likely be in violation of the prohibition against evasion in § 1033.201(a)(2).

One commenter was concerned that it would be difficult for a data provider to communicate to a consumer why a § 1033.331 denial occurred when the denial occurs before the data provider has authenticated the consumer's identity. Proposed § 1033.351(b)(3) would not have required a data provider to communicate why a denial has occurred before the data provider has authenticated a consumer's identity. If a data provider denies a request because the data provider has not authenticated the consumer, § 1033.351(d)(3)(ii) would simply require that, pursuant to reasonable policies and procedures, the data provider communicate that the data provider had not authenticated the consumer.

The CFPB understands that in limited cases, disclosure of the specific reason for a denial of access to an interface or for information on an interface might be prohibited by law or otherwise be inconsistent with compliance obligations or hinder law enforcement. Proposed § 1033.351(a) sought to provide flexibility to data providers in designing their policies and procedures regarding denials of information or interface access by providing in § 1033.351(a)

that policies and procedures must be "appropriate to the size, nature, and complexity of the data provider's activities."

The CFPB believes this language alone would have been sufficient to provide data providers flexibility to avoid acting in a manner inconsistent with legal obligations or effective law enforcement. However, given the nature of concerns in this context, the CFPB believes it will facilitate compliance to more clearly state in final § 1033.351(a) that a data provider has flexibility to design policies and procedures to avoid acting inconsistently with its other legal obligations, or in a way that could reasonably hinder enforcement against unlawful or potentially unlawful conduct. A reasonable policy and procedure designed to communicate the reasons for a denial of information or access would not mandate communication or disclosure of material that would require a data provider to violate the law or hinder law enforcement. For example, § 1033.351(b)(2) does not require a data provider to inform a third party that a "Suspicious Activity Report" was involved in a decision to deny information or interface access, because including such information could undermine ongoing and future law enforcement investigations by tipping off suspects or present other risks.

However, even if data providers have a legitimate basis not to communicate the reason for a denial, under § 1033.351(b)(2)(i) and (b)(3)(i) the data provider must create a record substantiating the basis for denial. For example, a data provider that denies a third party access pursuant to safety and soundness concerns, must create a record that substantiates the basis for the denial under § 1033.321(a). Under § 1033.351(d), the data provider's policies and procedures must account for retention of that record, but the final rule does not require that this record be disclosed to consumers or third parties. Denials of access or information present significant risks

of frustrating congressional intent, and § 1033.351(b)(2)(i) and (3)(i) helps ensure compliance with data providers' core obligation under the rule to make covered data available.

Policies and procedures for ensuring accuracy (§ 1033.351(c))

Under proposed § 1033.351(c)(1), the policies and procedures data providers would be required to establish and maintain by proposed § 1033.351(a) must be reasonably designed to ensure that covered data are accurately made available. Proposed § 1033.351(c)(2) listed elements that data providers would need to consider when designing their policies and procedures regarding accuracy, for example: (1) implementing the format requirements of proposed § 1033.311(b); and (2) addressing information provided by a consumer or a third party regarding inaccuracies in the covered data made available through its developer interface. Under proposed § 1033.351(c)(3), 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. The proposed rule explained that a qualified industry standard regarding accuracy is relevant to the reasonableness of a data provider's policies and procedures because it reflects the openness, balance, consensus, transparency, and other requirements of proposed § 1033.141.

The CFPB preliminarily determined that a data provider's policies and procedures should focus on the accuracy of transmission rather than the underlying accuracy of the information in the data provider's systems. The CFPB clarified that this means the policies and procedures should be designed to ensure that the covered data that a data provider makes available through its developer interface matches the information that it possesses in its systems. The CFPB explained that it was likely the data provider was already subject to several legal requirements regarding accuracy, such as Regulation E's protection of consumers against errors, and

Regulation Z's protection of consumers against billing errors. *See* 12 CFR part 1005; 12 CFR 1026.13. The CFPB sought comment on whether the final rule should include additional elements bearing on the reasonableness of a third party's policies and procedures regarding accuracy.

Few commenters expressed concerns regarding proposed § 1033.351(c). At least one bank trade association commenter, one research institute commenter and one Member of Congress supported the proposed rule's focus on the accuracy of transmission rather than the underlying accuracy of the information in the data provider's systems. The research institute commenter went further to say the CFPB should consider adding "accuracy testing" as an element of reasonableness for purposes of § 1033.351(c). A consumer advocacy group commenter recommended that the CFPB include dispute resolution requirements in § 1033.351(c), explaining that some regulatory regimes, such as the regulations enumerated in the proposal, have strict time limits for exercise of their dispute rights. Finally, a bank commenter opposed the reference to qualified industry standards in proposed § 1033.351(c)(3), stating that industry standard setting organizations are not well positioned to weigh in on the adequacy of accuracy policies and procedures, and generally have not done so to date.

For the reasons discussed herein, the CFPB is finalizing § 1033.351(c) as proposed with one terminology change. Section 1033.351(c) is authorized under CFPA section 1033(a) for the reasons stated above in the discussion of § 1033.351(a) as well as under CFPA section 1033(d). Policies and procedures for accuracy will promote the use and development of standardized formats by ensuring data providers are taking reasonable measures to share covered data in standardized formats. The CFPB has determined the mechanisms in part 1033, including the requirements in § 1033.311(b) with respect to standardized formats (discussed in part IV.C.3),

are sufficient to ensure data providers transmit information accurately. There is insufficient information in the current rulemaking record that establishes that more detailed procedures are necessary to resolve disputes regarding inaccurately transmitted covered data. The CFPB will monitor the market and engage in future rulemaking, as necessary.

With respect to the role of consensus standards in § 1033.351(c), recognized standard setters are well-suited to address the adequacy of accuracy policies and procedures. A consensus standard (as revised from the term qualified industry standard used in the proposal) regarding accuracy may be relevant to the reasonableness of a data provider's policies and procedures because it is produced through a process that takes into account the perspectives of all parties making available, receiving, and using covered data, consistent with the openness, balance, consensus, transparency, and other requirements of § 1033.141. Such standards, used in connection with accuracy policies and procedures, may indicate that covered data transmitted pursuant to an applicable consensus standard will be usable by authorized third parties.

Policies and procedures for record retention (§ 1033.351(d))

Proposed § 1033.351(d) would have provided that the policies and procedures required by § 1033.351(a) must be reasonably designed to ensure retention of records that are evidence of compliance with proposed subparts B and C of part 1033. The proposal's preamble explained that these requirements would give data providers flexibility to craft policies and procedures that are appropriate to the "size, nature, and complexity" of the individual data provider's activities, as required by proposed § 1033.351(a).The CFPB explained that this flexibility was intended to help data providers avoid conflicts with other legal obligations, manage data security risks, and minimize unnecessary impacts, consistent with the SBREFA Panel's recommendation.

Additionally, under proposed § 1033.351(d)(1), 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 to access a developer interface would have had to be retained for at least three years after a data provider has responded to the request. The CFPB explained that this duration would provide sufficient time to administer enforcement of proposed subparts B and C. The proposed rule also stated that all other records that are evidence of compliance with subparts B and C of part 1033 would need to be retained for a reasonable period of time.

To mitigate the risk that the flexibility of the record retention policies and procedures proposal might result in the absence of critical evidence of compliance, proposed § 1033.351(d)(2) identified examples records that would need to be retained. Proposed § 1033.351(d)(2) would have required that records retained pursuant to policies and procedures under proposed § 1033.351(a) include, without limitation: (1) records of requests for a third party's access to an interface, actions taken in response to such requests, and reasons for denying access, if applicable; (2) records of requests for information, actions taken in response to such requests, and reasons for not making the information available, if applicable; (3) copies of a third party's authorization to access data on behalf of a consumer; and (4) records of actions taken by a consumer and a data provider to revoke a third party's access pursuant to any revocation mechanism made available by a data provider. The CFPB requested comment on the types of records that should be retained, the length of the retention period, and the date from which the retention obligation should be measured.

Commenters generally supported the proposal. Some bank trade association commenters supported proposed § 1033.351(d)'s measuring of the retention period from the time of response, and at least one such commenter supported the proposed three-year retention period. Some data

provider commenters suggested that the retention period be for a shorter duration, such as two years, which they stated would be similar to the record retention requirements of Regulations E and Z and would reduce the amount of time records could be exposed to security risks. One trade association recommended that the final rule reduce the retention period applicable to responses to requests made through the developer interface. Some third party commenters recommended that the final rule include records of data providers' limitations of third party access, and that all communications of denials be submitted to the CFPB on a rolling basis. A trade association stated that retaining records on all third party requests would be unduly burdensome for data providers. Data provider commenters recommended that the final rule clarify that the provision does not require the retention of every login to the consumer interface or copies of data made available through the developer interface, explaining that such a retention would lead to significant costs. One bank commenter suggested that the final rule clarify what is meant by "copies of a third party's authorization" in proposed § 1033.351(d)(2)(iii). The commenter stated this could be interpreted by some data providers as a requirement to obtain and retain a copy of the full authorization disclosure provided by the third party to the consumer on the third party's own website or mobile application, which would be very hard for data providers to operationalize. Additionally, one trade association recommended that retaining records on all third party requests would be unduly burdensome for data providers. Further, some data provider commenters asserted that proposed § 1033.351(d) conflicts with CFPA section 1033(c), which provides that "[n]othing in [CFPA section 1033] shall be construed to impose any duty on a covered person to maintain or keep any information about a consumer."

For the reasons discussed herein, the CFPB is finalizing § 1033.351(d) with revisions to conform terminology and clarify the types of records to be retained, as well as revisions to specify the duration for which records should be retained pursuant to policies and procedures.

Retention period (§ 1033.351(d)(1))

Final § 1033.351(d)(1) provides that records that are evidence of a data provider's actions in response to a consumer's or third party's request for information or a third party's request to access a developer interface must be retained for at least three years after a data provider has responded to the request. All other records that are evidence of compliance with subparts B and C of part 1033 must be retained for a reasonable period of time of at least three years from the date of the action required under subparts B and C of part 1033.

Final § 1033.351(d)(1) revises the proposed language to the general obligation to clarify the nature of records to be retained pursuant to policies and procedures. The proposal described 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 to access a developer interface. The final rule contains new language clarifying that data providers must retain records "that are evidence of" a data provider's "actions in response to" a consumer's or third party's request for information or access to a developer interface." Including the phrase "evidence of" in the first sentence of § 1033.351(d)(1) is more consistent with the language used in the second sentence of that paragraph. For purposes of § 1033.351(d), relevant records are those that demonstrate overall fulfillment of requests for information. The final rule does not require retention of metadata related to individual consumer logins or activity on the consumer interface. Similarly, data providers do not need to retain copies of every request to the developer interface, or copies of data elements made available in response to each request, to the extent requests are fulfilled.

Section 1033.351(d)(1) must be read together with § 1033.351(a), which states, "[p]olicies and procedures must be appropriate to the size, nature, and complexity of the data provider's activities." For example, to the extent data providers fulfill consumer or third party requests, accurate aggregate data evidencing fulfillment, such as evidence of general availability of a consumer interface or a developer interface, would comply with § 1033.351(d). Of course, additional records would be necessary to the extent data providers do not make data available to consumers or third parties. For instance, if all or part of a consumer or developer interface is unavailable for a period of time to all consumers and third parties, data providers could retain records of the general unavailability of the interface. More detailed records will need to be retained to demonstrate maintenance of other policies and procedures requiring the creation of records, such as § 1033.351(b)(2)(i) and (b)(3)(i) with respect to records of denials of interface access and information requests. A data provider also might need to retain detailed information for some period of time as part of other policies and procedures required under § 1033.351. For instance, data providers might need to retain some information about responses to third party requests as part of maintaining accuracy-related policies and procedures pursuant to § 1033.351(c)(2)(ii).

Section 1033.351(d)(1) requires that records providing evidence of a data provider's actions in response to a consumer's or third party's requests for information and records of a third party's request to access a developer interface must be retained for at least three years after a data provider has responded to the request. The nature of the records retained will determine the most appropriate method of demonstrating compliance with this retention period.

In response to requests for clarity of the phrase "reasonable period of time" in the second sentence of § 1033.351(d)(1), final § 1033.351(d) includes new language specifying a more

concrete period. Final § 1033.351(d) states, "[a]ll other records that are evidence of compliance with subparts B and C of this part must be retained for a reasonable period of time of at least three years from the date of the action required under subparts B and C of this part." This aligns with the time period referenced in the first sentence with respect to responses to requests for information and access.

The CFPB believes a three-year record retention period set forth in § 1033.351(d)(1) is an appropriate duration to ensure retention of records that evidence compliance with data provider obligations under subparts B and C. Regulations E and Z, as codified in 12 CFR part 1005 and 12 CFR part 1026, respectively, implement EFTA and TILA, and the record retention requirements under Regulations E and Z offered for comparison by commenters are substantively different from that under § 1033.351(d). Records required under Regulation E and Regulation Z relate to regulated entities' disclosures to consumers pertaining to electronic fund transfers and consumer credit, respectively. Such disclosures to individual consumers are likely to be stale after a period of two years. Three years of records will allow for analysis of the patterns in a data provider's compliance with part 1033 over time. Moreover, based on the CFPB's supervisory and enforcement experience, a three-year retention period is an appropriate amount of time to enable the CFPB and other enforcement agencies to examine or conduct enforcement investigations. A shorter record retention period would make it more difficult to ensure that the necessary records are available.

The CFPB is issuing final § 1033.351(d) pursuant to CFPA section 1022(b)(1), which authorizes the CFPB to prescribe rules as may be necessary or appropriate to enable the CFPB to administer and carry out the purposes and objectives of the Federal consumer financial laws, including carrying out the objectives of CFPA section 1033, and to prevent evasions thereof.

Section 1033.351(d) will assist the CFPB and other enforcement agencies with administering CFPA section 1033 by ensuring records are available to evaluate compliance with data providers' obligations under the rule. CFPA section 1033(c) does not indicate otherwise, for two independent reasons. First, § 1033.351(d) is a rule issued pursuant to CFPA section 1022(b)(1), while section 1033(c) is a rule of construction concerning "this section," *i.e.*, CFPA section 1033. Second, § 1033.351(d) does not require data providers to keep records "about a consumer." Rather, it requires data providers to establish policies and procedures to maintain records related to their compliance with part 1033.

Final § 1033.351(d) does not override congressional intent with respect to CFPA section 1033(b)(4) or (c). Final § 1033.351(d) only requires records providing evidence of compliance with subparts B and C of part 1033, and pursuant to § 1033.221, data providers are not required to make available any covered data that falls under the statutory exceptions at CFPA section 1033(b). Nor does § 1033.351(d) require data providers to maintain the underlying covered data that must be made available pursuant to CFPA section 1033(a).

Certain records retained pursuant to policies and procedures (§ 1033.351(d)(2))

As proposed, final § 1033.351(d)(2) provides, "Records retained pursuant to policies and procedures required under paragraph (a) of this section must include" categories enumerated in subsequent paragraphs, "without limitation." The CFPB is finalizing the enumerated categories under § 1033.351(d)(2) with revisions to clarify the types of records to be retained, and other revisions to clarify how the three-year period in § 1033.351(d)(1) applies to those records. In response to questions about the types of records required and to conform to language in final § 1033.351(d)(1), some provisions refer to requiring records "providing evidence of" certain activity, discussed below. To provide greater clarity on how the three-year time period applies to

the requirements of subparts B and C, final § 1033.351(d) includes additional categories of records that a data provider's policies and procedures must include and how the three-year period applies, as discussed below.

Final § 1033.351(d)(2)(i) specifies records documenting requests for a third party's access to an interface, actions taken in response to such requests, and reasons for denying access, if applicable, for at least three years after the data provider has responded to the request. Proposed § 1033.351(d)(2)(i) specified that data provider policies and procedures must include "records of" requests for a third party's access to an interface, actions taken in response to such requests, and reasons for denying access, if applicable; and did not specify a retention period.

Final § 1033.351(d)(2)(i) revises this language to clarify that data providers' policies and procedures must include records "documenting" requests for third party access, actions taken, and reasons for denying access, if applicable. The term "documenting" is intended to clarify that policies and procedures must be designed to capture documentary evidence of requests to access the interface, and can include but does not require retention of actual copies of information. The CFPB is making this revision in light of how consequential granting access to a third party is, with respect to the number of consumers potentially affected by the decision, the risks of pretextual denials, and the complex factors involved in granting access, as discussed in part IV.C.4 with respect to § 1033.321. The final rule also includes new language clarifying how the three-year period applies to these records. Records documenting decisions around onboarding will be particularly important for enforcement of §§ 1033.201 and 1033.321.

Final § 1033.351(d)(2)(ii) specifies records providing evidence of fulfillment of requests for information, actions taken in response to such requests, and reasons for not making the information available, if applicable, for at least three years after the data provider has responded

to the request. Proposed § 1033.351(d)(2)(ii) would have required a data provider's policies and procedures to include "records of" requests for information, actions taken in response to such requests, and reasons for not making the information available, if applicable; and did not specify a retention period. The final rule revises the language with respect to requests for information to records "providing evidence of fulfillment of requests." This revision is intended to clarify the scope of records required, as discussed above with respect to § 1033.351(d)(1).

Final § 1033.351(d)(2)(iii) specifies records documenting that the third party has followed the authorization procedures in § 1033.401 to access data on behalf of a consumer, for at least three years after such records are generated. Proposed § 1033.351(d)(2)(iii) would have required data provider policies and procedures to include "[c]opies of a third party's authorization to access data on behalf of a consumer," and would not have specified a retention period. The final rule revises that language to refer to "[r]ecords documenting that the third party has followed the authorization procedures," to conform to the language in § 1033.331(b)(1)(iii). The final rule recognizes that, by virtue of its transmission to the data provider through the developer interface, the authorization disclosure received by the data provider might not be identical to the form received by the third party.

Final § 1033.351(d)(2)(iv) specifies records providing evidence of actions taken by a consumer and a data provider to revoke a third party's access pursuant to any revocation method made available by a data provider, for at least three years after the revocation. Proposed § 1033.351(d)(2)(iv) would have required data provider policies and procedures to include "records of" actions taken by a consumer and a data provider to revoke a third party's access pursuant to any revocation "mechanism" made available by a data provider; and would not have specified a retention period. Final § 1033.351(d)(2)(iv) uses the phrase "records providing

evidence of" to clarify that identical records are not required. In addition, § 1033.351(d)(2)(iv) uses the term "method" rather than "mechanism," to conform this provision to final § 1033.331(e).

The final rule also specifies in § 1033.351(d)(2) three categories of records that would need to be retained for a three-year period: evidence of commercially reasonable performance specifications (§ 1033.351(d)(2)(v)), written policies and procedures required under § 1033.351 (§ 1033.351(d)(vi)), and disclosures made under proposed § 1033.341 (§ 1033.351(d)(2)(vii)). Although the proposal did not specify that data providers' policies and procedures regarding recordkeeping include these records, proposed § 1033.351(d)(2) indicated that the records specified were not exhaustive. As noted above, proposed § 1033.351(d) stated that "[t]he policies and procedures required by paragraph (a) of this section must be reasonably designed to ensure retention of records that are evidence of compliance with subparts B and C of this part." Proposed § 1033.351(d)(2) stated that records retained pursuant to policies and procedures required under paragraph (a) of this section must include, "without limitation," certain categories of records.

Final § 1033.351(d)(2)(v) specifies records of commercially reasonable performance described in § 1033.311(c)(2)(C)(ii), for at least three years after the period recorded, which will enable enforcement and supervision of final § 1033.311(c). Final § 1033.351(d)(2)(vi) specifies written policies and procedures required under § 1033.351 for three years from the time such material was last applicable. And final § 1033.351(d)(2)(vii) specifies disclosures required under § 1033.341, for three years from the time such material was disclosed to the public.

A commenter's suggestion to explicitly require data providers to keep records that demonstrate justification for limiting third party access is already covered in the rule. As

proposed, final § 1033.351(d)(2)(ii) requires policies and procedure to create "[r]ecords of requests for information," as well as the "actions taken in response to such requests." The final rule does not require data providers to report access denials monthly. Such a requirement would be burdensome without significant additional benefit. Data providers must have policies and procedures to substantiate reasons for denying access under § 1033.351(b) and the CFPB believes administrative enforcement and supervision will be sufficient to monitor compliance.

D. Subpart D—Authorized Third Parties

1. Overview

Subpart D establishes authorization procedures and obligations for third parties seeking to access covered data from data providers pursuant to the final rule's framework. The authorization procedures require a third party to obtain the consumer's express informed consent to the third party's access of the consumer's covered data. The third party must provide the consumer with an authorization disclosure that meets certain content and other requirements set forth in subpart D. Among other things, the authorization disclosure must include a statement whereby the third party certifies that it will meet the third party obligations set forth in subpart D, including limits on the third party's collection, use, and retention of the consumer's covered data. Subpart D also includes specific requirements that apply when the third party is using a data aggregator, and policy and procedure requirements related to record retention that apply if the third party is also a covered person or service provider pursuant to the CFPA.

Similar to the final rule, the proposed rule would have included authorization procedures and third party obligations designed to ensure that third parties accessing covered data pursuant to the rule's framework are acting on behalf of the consumer whose covered data are being accessed. It would have also included specific requirements that apply when a third party is using

a data aggregator and policy and procedure requirements related to retaining evidence of compliance. A wide variety of commenters, including data providers, third parties, research institutes, consumer advocates, and a Member of Congress, generally supported the proposed approach to authorized third party data access in subpart D. As discussed below, other commenters expressed concerns about the proposed approach, including concerns related to the CFPB's legal authority.

Legal authority

Some commenters asserted that the CFPB lacks the legal authority for some or all of the provisions in proposed subpart D. Specifically, a law firm commenter described authorized third parties as consumers' agents and asserted that the CFPB lacks authority to prescribe how consumers authorize agents to access data or how agents later use that data. A trade association for nondepositories argued that the third party obligations should not limit a third party's collection and use of covered data. This commenter argued that the proposed rule conflicted with traditional agency law, which permits an agent to take an action that does not necessarily benefit the principal.[83] They further contended that the proposed rule would impermissibly override consumers' choices regarding how third parties authorized to receive data may later use that data.

Other commenters criticized subpart D but for opposite reasons. Specifically, these commenters argued that the proposed approach exceeded the CFPB's authority because it would give an overly broad set of third parties access to covered data. According to one third party commenter, the term "representative" should be read as similar to, and connected with, "agent" and "trustee" in accordance with the interpretive canon that "a word is known by the company it

[83] This commenter cited the Restatement (Third) of Agency (2006).

keeps" and the canon that when "a more general term follows more specific terms in a list, the general term is usually understood to embrace only objects similar in nature to those objects enumerated by the preceding specific words."[84] According to this commenter, representatives must have a fiduciary relationship with the consumer similar to a principal-agent and trustor-trustee relationship.[85] The commenter argued that it would be inappropriate to allow entities that deal with consumers at arm's length in the marketplace and are not in a fiduciary relationship with the consumer to act as authorized third parties. Similarly, two trade associations for credit unions asserted that third party access on behalf of a consumer should be limited to situations where the third party and consumer have a legal relationship that necessitates the access.

As discussed in more detail below in part IV.D.4 regarding third party obligations, some commenters asserted that the CFPB lacked authority regarding certain proposed limits on an authorized third party's use of covered data.

After considering the comments discussed above as well as other relevant comments discussed throughout part IV.D, the CFPB has determined that the provisions in subpart D align with congressional intent and are within the CFPB's rulemaking authority. The plain language of CFPA section 1033(a) provides that, subject to rules prescribed by the CFPB, a covered person shall make available to a "consumer," upon request, certain information in the control or possession of the covered person. CFPA section 1002(4) defines "consumer" as "an individual or an agent, trustee, or representative acting on behalf of an individual." [86] For convenience, part

[84] The commenter quoted *Dubin v. United States*, 599 U.S. 110 (2023), and *Epic Sys. Corp. v. Lewis*, 584 U.S. 497 (2018).

[85] The commenter cited the Restatement (Third) of Agency (2006) and also the Restatement (Third) of Trusts (2003).

[86] For example, Merriam Webster defines "on behalf of" to mean "in the interest of." https://www.merriam-webster.com/dictionary/on%20behalf%20of.

1033 generally refers to the individual as the "consumer" and an agent, trustee, or representative acting on behalf of that individual as an "authorized third party." As noted elsewhere, the substance of the rule aligns with the CFPA's definition of consumer, and nothing in the CFPA prevents the CFPB from using different vocabulary within the rule.

The provisions in subpart D are designed to ensure that, consistent with carrying out the objectives of CFPA section 1033, consumers provide informed consent to third parties that access covered data pursuant to the final rule's framework, that consumers retain control over third parties' access, and that third parties act on behalf of consumers when collecting, using, and retaining covered data pursuant the final rule's framework. Accordingly, the final rule requires third parties accessing covered data pursuant to the final rule's framework to adhere to the authorization procedures and third party obligations in subpart D, including the specific requirements for data aggregators (as applicable). These authorization procedures and third party obligations ensure that third parties accessing a consumer's covered data are acting on the consumer's behalf. They ensure the consumer is effectively informed about and has provided meaningful consent for the third party's collection, use, and retention of the consumer's covered data, and that the consumer retains the ability to control access to that covered data. The authorization procedures and third party obligations also ensure that the third party's access to covered data accords with the consumer's intent and reasonable expectations and is for the consumer's benefit.

As noted above, commenters relied upon an analogy between the definition of "consumer" in CFPA section 1002(4) and agency law, but they drew opposite conclusions from that analogy. The final rule establishes that a third party has a duty to act for the principal's benefit in its collection, use, and retention of data, which is in line with well-established

principles of agency law. Under agency law, an agent is required to subordinate the agent's interests to those of the principal and to place the principal's interests first on all matters connected with the agency relationship.[87] Similarly, here, the final rule limits third party collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service. Furthermore, as a commenter indicated, agency law does sometimes permit a principal to consent to conduct by an agent that would otherwise breach the agent's duties to the principal, but only if the consent is the product of an adequately informed judgment by the principal.[88] Likewise, as explained below, the final rule permits third parties to access covered data for certain purposes, including targeted advertising, cross-selling of other products or services, and data sales, if data access for these purposes are separately authorized as a standalone product or service. Including those purposes as part of an authorization for the consumer's requested product or service would run contrary to the third party's obligations to the consumer. However, where the consumer affirmatively requests targeted advertising, cross-selling of other products and services, or data sales, the third party can obtain meaningful consent through a separate authorization for a standalone product or service. Thus, the final rule is consistent with common law agency principles.

The CFPB does not agree with some commenters that the effect of subpart D is to override consumers' choices. Instead, subpart D establishes a framework to ensure that consumers have a meaningful opportunity to understand and consent to uses of data on their behalf. The evident congressional purpose of CFPA section 1033(a) is to give consumers greater control of data concerning their financial accounts, and this purpose would be fatally undermined

[87] *See* Restatement (Third) of Agency section 8.01 (2006).

[88] *See id.* section 8.06 and section 8.06 cmt. b.

if third parties could use the data in ways that consumers would not expect and would reject if given an unobstructed choice. As part of its rulemaking role assigned by Congress, the CFPB has crafted a framework in subpart D to ensure that consumers are able to make informed choices.

The CFPB does not agree with other commenters that suggest that only a narrow class of certain fiduciaries should be recognized as authorized third parties. The CFPB has framed subpart D precisely to ensure that covered data are available only to agents, trustees, and representatives acting on behalf of the consumer. Regardless of whether entities engaged in the current open banking system would qualify for that category, if an entity satisfies the final rule's conditions—including the obligations to act on behalf of the consumer—it is appropriate to recognize it as an authorized third party.

Accordingly, subpart D is consistent with CFPA section 1033 and with the definition of "consumer" in CFPA section 1002(4). Moreover, even assuming for the sake of argument that commenters' narrower or broader readings of CFPA section 1002(4) were accepted, the CFPB notes that Congress has conferred express rulemaking authority on the CFPB in CFPA section 1033(a) and has done so in broad terms. Because all data sharing under section 1033 of the CFPA is "[s]ubject to rules prescribed by the Bureau," the CFPB has authority to place conditions on data access in order to carry out CFPA section 1033 and realize its objective of meaningful consumer control of the data that is shared pursuant to the statute.

Finally, although commenters did not specifically challenge the basis for the proposed provision requiring certain third parties to establish and maintain policies and procedures for record retention, this provision is authorized under CFPA sections 1022(b)(1) and 1024(b)(7), as discussed in part IV.D.6.

Other concerns related to the proposed approach to authorizing third party data access

Some commenters raised concerns with the general approach to third party access to covered data in proposed subpart D. As further discussed elsewhere in this part IV.D, the CFPB concludes that the general approach to third party access to covered data in subpart D of the final rule, including the authorization procedures and third party obligations, best aligns with congressional intent to ensure that third parties accessing covered data are acting on behalf of consumers. Additional discussion of these comments and the rationale for the CFPB's determination can be found in the remainder of this part IV.D as well as in the *General Comments Received on the Proposal* discussion of part IV and in part IV.C.5.

Some data providers and trade associations for data providers stated that the rule should mandate that third parties certify that they accept liability in certain circumstances, are adequately capitalized, and carry sufficient indemnity insurance to fulfill their liability obligations. However, the purpose of the third party obligations in subpart D is to ensure that third parties accessing covered data are doing so on the consumer's behalf. Content related to the allocation of liability between data providers and third parties would be outside the scope of this purpose. This is also the case for capitalization and indemnity insurance requirements.

A bank commenter suggested that once the rule becomes effective, it should apply to covered data currently held by third parties, to ensure that data are uniformly and consistently protected. However, the third party authorization procedures in subpart D provide procedures and obligations for third parties seeking to access covered data pursuant to the final rule's framework. As such, the final rule does not apply to covered data accessed by third parties prior to the final rule's effective date.

Third party access outside the subpart D framework

Two trade associations representing nondepository entities commented that the CFPB should clarify that the rule does not prohibit third parties from accessing covered data outside the rule's data access framework. One of these trade association commenters stated that the scope of CFPA section 1033 is limited and does not authorize the rule to prohibit third parties from obtaining a consumer's financial information outside the rule's framework. The commenter requested that the CFPB clarify that the rule does not establish the exclusive means for a third party to obtain covered data and does not impose restrictions on third parties that access such data without relying on the CFPA section 1033 access right. Another bank commenter stated the rule does not address how it affects existing contracts providing for access to consumer financial data and recommended that the CFPB provide for the grandfathering of such contracts.

Several bank commenters and bank trade association commenters stated that the rule's protections should apply to third parties attempting to access covered data, even if those third parties do not attempt to become authorized third parties and rely on the rule's framework to obtain access to covered data. They stated that third parties could evade the rule's protections by declining to become authorized third parties, by not trying to access covered data through the rule's framework, and by relying on other methods to access covered data.

CFPA section 1033 provides consumers, and third parties acting on behalf of consumers, with a right to access their data, and the rule creates a framework to implement that right. The CFPB expects that third parties and covered data providers will employ the rule's framework for arranging third party access to covered data authorized by the consumer. The CFPB has determined that the rule's framework will provide significant benefits to data providers, third parties, and consumers. Data providers will receive assurance that third parties have

authorization from the consumer to access data and a commitment from third parties that they will comply with certain consumer protections and other obligations, which will promote data minimization and sound risk management. Moreover, as noted above, the CFPB would not consider data providers under this final rule to be furnishers solely by virtue of permitting data access pursuant to an authorization that is consistent with the final rule. Third parties seeking to access covered data on behalf of consumers to provide products or services generally will receive that access if they comply with the authorization procedures and other conditions of the rule. Most importantly, the rule will provide significant protections to consumers by ensuring that third parties are accessing covered data on behalf of consumers—as the CFPA envisions—and are taking appropriate steps to protect their covered data. The rule does not address the topic of any data sharing outside the rule's framework, including through existing contracts. However, the prohibitions in the CFPA against unfair, deceptive, or abusive acts or practices will bear on any claimed effort to proceed outside of the safe, secure, reliable and competitive open banking framework that is enabled by this final rule. The CFPB will closely monitor the market to determine whether attempts to arrange for consumer authorized access to covered data outside the framework constitute unfair, deceptive, or abusive acts or practices.

Screen scraping by third parties

In the proposal, the CFPB expressed the goal of transitioning the market away from screen scraping and noted the nearly universal consensus that developer interfaces should supplant screen scraping. The proposed rule also discussed the overcollection, data security, accuracy, and infrastructural burden concerns related to screen scraping. As discussed in part IV.C.3 above, to facilitate a transition, the CFPB proposed to prevent data providers from relying on screen scraping as a means of enabling third parties to access consumer data, even though it

did not formally prohibit screen scraping. The CFPB did not propose requiring that data providers permit screen scraping as an alternative method of access, such as to address unavailability when the data provider's system interface is down for maintenance. The proposed rule explained that screen scraping generally presents risks to consumers and the market and that relying on credential-based screen scraping would complicate the mechanics of data access, particularly with respect to authentication and authorization procedures.

Several commenters addressed screen scraping by third parties. Some data provider and data provider trade association commenters asked the CFPB to prohibit third parties from screen scraping or to require third parties to include commitments to avoid screen scraping in their certification statements. These commenters generally stated that screen scraping can be difficult for data providers to identify and prevent. According to these commenters, detecting and preventing screen scraping requires significant resources even for large banks, and cannot be accomplished with certainty. Given the risks involved in screen scraping, these commenters stated, the obligation to prevent it should rest with the third party, which is most directly able to control the practice.

Several commenters tied their concerns regarding screen scraping to the coverage of the rule. For example, several data providers and trade associations for data providers stated that because the proposal would not require all third parties to access data through the developer interface, and would apply only to covered data, some third parties could still attempt to screen scrape outside the scope of the rule. One bank commenter stated that third parties that scrape non-covered data could easily scrape covered data at the same time. A data aggregator commenter asked for clarity on the use of screen scraping for non-covered data or when developer interfaces are unavailable.

Several other commenters suggested that the incentive to access data through a developer interface might be insufficient to channel data flows through the framework in the proposed rule. For example, a researcher and a service provider commenter stated that screen scraping persisted in Australia and Europe despite the development of API access. One of these commenters asserted that poor API quality caused the persistence of screen scraping in Australia, while the other claimed that the lack of a ban on screen scraping was responsible for the continuation of the practice in Europe.

In contrast, several commenters, mainly third parties and nonprofit organizations, recommended that the final rule expressly permit screen scraping in limited circumstances. These commenters generally suggested two circumstances to permit screen scraping: (1) when developer interfaces are unavailable; and (2) when data made available through developer interfaces is unreliable. A few commenters recommended allowing screen scraping until data providers have established developer interfaces. A nonprofit organization commenter suggested that the possibility of screen scraping would serve as a check on anticompetitive conduct by data providers and a way of incentivizing developer interface quality. Another nonprofit organization commenter recommended allowing tokenized screen scraping as a more secure alternative to traditional screen scraping. A researcher commenter stated that any prohibition on third parties using consumer credentials to access developer interfaces risked leaving third parties without means of accessing data if the interface is unavailable. A nonprofit organization commenter stated that screen scraping might be the only means of accessing non-covered data from some data providers. Finally, some community banks, credit unions, and related trade association commenters also requested that the final rule permit screen scraping. These commenters

generally believed that data providers should have the flexibility to permit screen scraping by trusted third parties instead of enabling access through developer interfaces.

Conversely, many large data providers and trade associations for data providers opposed any screen-scraping exception. These commenters generally stated that any fallback option for screen scraping would create the same consumer transparency, control, security, and privacy risks the proposal was trying to avoid. Finally, some community banks, credit unions, and related trade association commenters also requested that the final rule permit screen scraping. These commenters generally believed that data providers should have the flexibility to permit screen scraping by trusted third parties or build developer interfaces.

The CFPB has determined that specifically prohibiting third parties from screen scraping when they obtain covered data through the final rule, or requiring them to make a certification to that effect, is unnecessary. The final rule's authorization and authentication requirements do not accommodate data access arrangements in which a third party retains consumers' access credentials. And the final rule imposes limitations on the collection, use, and retention of covered data that third parties could not feasibly meet through screen scraping.

Once data providers have enabled the safe, secure, and reliable forms of data access envisioned in this rule, the CFPB cautions that screen scraping attempts by third parties to reach data covered by such arrangements could well be limited by the CFPA's prohibition on unfair, deceptive, and abusive acts or practices.[89] As discussed throughout this document, screen scraping poses risks to consumer privacy and data security. The CFPB understands that in some circumstances, screen scraping may be the only practical means by which third parties can access consumer data. For example, a third party might seek to access non-covered data or data held by

[89] *See* 12 U.S.C. 5531.

a financial institution that has not established a developer interface. But if a third party attempts to screen scrape consumer data when a more secure, structured alternative means of access is available, such as the developer interface or a substantially similar interface, then the third party would be needlessly exposing consumers to harm. Depending on the facts and circumstances, such activity might well constitute an unfair, deceptive, or abusive act or practice.

Finally, the CFPB has decided against providing for screen scraping as a fallback means of third party access under the final rule. The final rule attempts to reduce the risks of screen scraping by facilitating the market's transition toward more secure methods of consumer-authorized data access. Providing for screen scraping as an alternative method of data access would undermine this important goal. Certain technologies, such as tokenized screen scraping, could mitigate some of the risks of credential-based screen scraping. But even tokenized screen scraping would not alleviate the risks to privacy and accuracy, or meaningfully advance the statutory mandate to promote the development and use of standardized formats.

Regarding concerns that the absence of a screen-scraping alternative might leave consumers without a means of authorizing access to their covered data, the CFPB has determined that the performance standards for developer interfaces will ensure that consumers and third parties have reliable access to covered data. To the extent that such access is interrupted by maintenance or reliability issues, it is not clear that screen scraping would serve as a practical alternative. If third parties collected consumer credentials in advance of a potential availability issue, the resulting mass accumulation of consumer credentials by third parties would effectively undermine the final rule's efforts to encourage safer and more structured means of data access. But waiting until the developer interface is unavailable might also be impractical because the

sudden request for credentials might confuse consumers, and the unavailability might extend to the interface the third party seeks to screen scrape.

To the extent that small data provider commenters viewed screen scraping as a way to alleviate the burden of implementation, the CFPB has provided alternative means of reducing burden on small entities. For example, part IV.C.3 discusses how data providers may use service providers that rely on screen scraping to facilitate access to the developer interface. And part IV.A.5 discusses the tiered compliance dates designed to ease the burden on smaller data providers.

2. Third party authorization procedures (§ 1033.401)

Proposed § 1033.401 specified what requirements a third party would have to satisfy to become an authorized third party entitled to access covered data on behalf of a consumer. The CFPB preliminarily determined that these proposed requirements would, among other things, help ensure that a consumer understands and would be able to exercise control over what covered data the third party would collect and how it would be used. The CFPB also preliminarily determined that the proposed procedures would help ensure that the third party would take appropriate steps to protect the consumer's data and that the consumer would provide express informed consent for the third party to collect, use, and retain the covered data. The CFPB preliminarily determined that these requirements would help ensure that a third party accessing covered data is doing so on behalf of a consumer and not for the third party's own benefit, consistent with the definition of consumer in CFPA section 1002(4) and as used in section 1033.

Proposed § 1033.401 would have provided that, to become an authorized third party, the third party must seek access to covered data from a data provider on behalf of a consumer to

provide a product or service the consumer requested. This proposed requirement was intended to ensure that the third party is acting on behalf of the consumer—by accessing covered data to provide the product or service requested by the consumer—and is not seeking access to covered data for its own purposes.

Proposed § 1033.401 also provided that a third party would have to satisfy the prescribed authorization procedures to become an authorized third party. Under proposed § 1033.401, the three-part authorization procedures would require a third party to: (a) provide the consumer with an authorization disclosure as described in proposed § 1033.411; (b) provide a statement to the consumer in the authorization disclosure, as provided in proposed § 1033.411(b)(5), certifying that the third party agrees to the obligations described in proposed § 1033.421; and (c) obtain the consumer's express informed consent to access covered data on behalf of the consumer by obtaining an authorization disclosure that is signed by the consumer electronically or in writing.

The proposed requirement in § 1033.401(a) that a third party provide an authorization disclosure to the consumer was intended to help ensure that the consumer understands the key terms of access and can make an informed decision about whether to grant the third party access to the consumer's financial data. The proposed requirement in § 1033.401(b) that a third party provide a statement to the consumer certifying that the third party will comply with certain obligations would help ensure that the third party is acting on behalf of the consumer in accessing the covered data. The proposed requirement in § 1033.401(c) that the third party obtain the consumer's express informed consent to access covered data would ensure that the consumer has agreed to allow the third party to access that data on the consumer's behalf.

As discussed above in connection with § 1033.331(d), the CFPB proposed that a data provider that receives a request for covered data from a consumer that jointly holds an account or

from an authorized third party acting on behalf of such a consumer must provide covered data to that consumer or authorized third party. Consistent with that proposed approach, for a jointly held account, a third party would have to comply with the third party authorization procedures in proposed § 1033.401 for the joint account holder on whose behalf the third party is requesting access. The CFPB requested comment on whether other account holders should receive authorization disclosures or otherwise be notified, or should have an opportunity to object, when an account holder authorizes a third party to access covered data from a jointly held account.

The CFPB also requested comment on whether the authorization procedures in proposed § 1033.401 would be sufficient to ensure that a third party is acting on behalf of a consumer in obtaining access to covered data or whether the CFPB should consider alternative procedures. The CFPB additionally requested comment on whether the authorization disclosure, including the statement that the third party will comply with certain third party obligations, would be sufficient to ensure that the consumer would be able provide express informed consent for the third party to access covered data on behalf of the consumer. The CFPB requested comment on whether the rule should include other protections or clarifications, such as express prohibitions on false or misleading representations or omissions to induce the consumer to consent to the third party's access to covered data.

Additionally, the CFPB proposed in § 1033.401 to apply a consistent set of procedures to all third parties attempting to access covered data. The CFPB requested comment about whether there are certain third parties, such as smaller or non-commercial parties, for which proposed § 1033.401 would not be appropriate. The CFPB also requested comment about whether the authorization procedures described in proposed § 1033.401 should be streamlined for certain third parties. In addition, the CFPB requested comment on whether there are certain

circumstances involving the transmission of data to third parties for which proposed § 1033.401 would not be appropriate. Finally, to help the CFPB assess the need for potential exemptions to proposed § 1033.401, the CFPB requested comment on how individuals who are not account owners currently use existing legal mechanisms to directly access covered data.

Several nondepository entity commenters supported the proposed authorization procedures. One stated that the proposed authorization procedures will help consumers understand and consent to third parties accessing their data and that the procedures are sufficiently clear and flexible.

Commenters generally did not oppose the three-step authorization procedures, but some commenters recommended certain revisions or clarifications. One nondepository entity commenter urged the CFPB to consider streamlined authorization procedures when the consumer already has authorized access and is seeking to change the authorization by, for example, giving access to more or less data or permissioning data to additional parties. A bank trade association commenter recommended that the CFPB clarify the third party authorization procedures when material terms in the authorization change, such as when aspects of the requested product change, additional data are needed, or the service provider or data aggregator changes. This commenter urged the CFPB to require new disclosures and a new authorization when material terms in the authorization change. A trade association commenter stated that it was unclear whether third parties are required to comply with the proposed certification, disclosure, and use limitation requirements for non-covered data.

Several commenters stated that data providers should play a more significant role in the third party authorization process. Several commenters, including banks and a trade association, maintained that data providers, rather than third parties, are best positioned to obtain consumers'

authorizations. A trade association commenter stated that data providers hold consumers' accounts and have account verification and access procedures to verify consumers' requests.

Several commenters addressed whether, as part of the authorization procedures, the rule should impose regulatory obligations directly on third parties, including data aggregators. Several bank and bank trade association commenters recommended that the rule impose obligations directly on third parties, rather than requiring them to certify that they will abide by certain obligations as a condition for becoming authorized to access covered data. These commenters raised concerns about how the obligations would be enforced against third parties. They also stated that the CFPB should supervise third parties, particularly data aggregators, to ensure that they comply with the third party obligations in the rule.

Several commenters recommended that the rule include additional consumer protections. A consumer advocate commenter requested that the CFPB consider additional provisions to ensure that consumers provide express informed consent for third parties accessing covered data. That commenter recommended that the rule include prohibitions on false or misleading representations to induce the consumer to provide consent to the third party's access to the consumer's covered data. Another consumer advocate commenter recommended additional consumer protections, including requiring privacy impact statements and authorizing private rights of action for consumers to pursue penalties that violate third party obligations. A consumer advocate commenter and a data aggregator commenter recommended that the privacy protections apply to any parties subject to the rule. Finally, a consumer advocate commenter suggested that the CFPB require a waiting period of fourteen days before allowing third parties to solicit any additional products or services or at least before requesting authorization for certain additional uses, like debt collection, marketing for harmful high-cost credit products, and others.

A bank trade association requested that the rule clarify that a consumer's electronic signature on an authorization disclosure is intended to comport with the ESIGN Act. One commenter suggested that the rule should permit "clear affirmative consent." This commenter asked that the rule clarify that a clear affirmative action that a consumer takes on a digital interface, such as clicking "Agree" or "Continue," after being presented with the authorization disclosure, would satisfy the requirement that an authorization disclosure be signed electronically. The commenter suggested that "full electronic signatures" are an unusual method of obtaining express informed consent on a digital interface, such as an internet browser or application, would be inconsistent with seeking innovative products and services, and could create a barrier for consumers. Another commenter requested that the rule confirm a third party may rely on "click through acceptance" of the authorization disclosure and suggested that clicking "agree" or "proceed" should satisfy the express informed consent requirement. Conversely, a consumer advocate commenter suggested that the rule not permit the use of click through boxes and suggested toggles for "on/off" authorization.

Several commenters addressed how the authorization procedures should function for joint accounts. These comments are described in part IV.C in connection with the discussion of § 1033.331(d).

Several commenters addressed whether the authorization procedures should apply to all third parties or whether there should be exceptions for certain third parties, such as smaller third parties or non-commercial third parties. A bank trade association commenter stated that data providers already have procedures for providing information to natural third parties, such as agents, attorneys, accountants, and guardians. This commenter argued that such individuals should not be required to go through a developer interface, and that the rule should exempt

natural third parties. A consumer advocate commenter stated that the CFPB should consider whether there should be exceptions for verified non-commercial third parties, such as family members or nonprofit counselors, that may need read-only access to data to help consumers manage their finances. Another consumer advocate commenter and a bank commenter recommended that the rule not provide any exceptions for third parties. The consumer advocate commenter stated that there may be situations in which non-commercial users, such as executors or guardians, should be able to access covered data through a consumer interface.

For the reasons discussed herein, the CFPB is finalizing the three-step authorization procedures as proposed. To become an authorized third party, under proposed § 1033.401, a third party must: (a) provide the consumer with an authorization disclosure as described in § 1033.411; (b) provide a statement to the consumer in the authorization disclosure certifying that the third party agrees to certain obligations described in § 1033.421; and (c) obtain the consumer's express informed consent to access covered data on behalf of the consumer by obtaining an authorization disclosure that is signed by the consumer electronically or in writing.

The CFPB has determined that the authorization procedures, as described in more detail below, appropriately ensure that a third party accessing covered data pursuant to the rule is doing so on behalf of a consumer and not for the third party's own benefit, consistent with the definition of consumer in CFPA section 1002(4) and used in section 1033. The authorization procedures will help ensure that a consumer understands and can exercise full control over what covered data the third party collects and how that data will be used. The authorization procedures also will help ensure that consumers are not unknowingly or reluctantly acquiescing to forms of data access that they do not want. In addition, the authorization procedures will help ensure that the third party will take appropriate steps to protect the consumer's data and that the consumer

provides express informed consent for the third party to collect, use, and retain the covered data. The authorization procedures clearly apply only to third parties that are attempting to access covered data through the rule's framework and the CFPB has concluded that additional clarification is not needed to specify that the authorization procedures do not apply when entities are attempting to access non-covered data.

As noted above, some commenters recommended that data providers play a larger role in the authorization process and have primary responsibility for consumer authorizations. The CFPB has determined that it is appropriate for third parties to obtain consumer authorization for third party access to covered data. The third party is providing the product or service to the consumer and understands what covered data are reasonably necessary for providing that product or service. Assigning responsibility for consumer authorization to the data provider could create friction and impair access to covered data by authorized third parties. The third party authorization procedures ensure that third parties are acting on behalf of consumers and that consumers understand and maintain control over third party access to their covered data. While the third party is responsible for obtaining the consumer's authorization, as discussed in part IV.C.5, a data provider must make available covered data when it receives certain information, including, as provided in § 1033.331(b)(1)(iii), information sufficient to document the third party has followed the § 1033.401 authorization procedures.

The CFPB has concluded that streamlined authorization procedures would not be appropriate when the consumer or authorized third party seek to change the terms of the authorization, such as to expand or narrow the scope of access to covered data. When the parties seek to change the terms of the authorization, the authorized third party must obtain a new

authorization to ensure that the consumer understands and provides express informed consent for new terms for the authorized third party's access to covered data.

The CFPB also has concluded that the approach in § 1033.401(b) to require third parties to certify to abide by certain obligations related to the data access is appropriate. As part of the authorization procedures, third parties must certify to consumers that they will comply with certain obligations as condition of becoming authorized third parties entitled to access covered data on behalf of consumers. Similarly, data aggregators also must certify to consumers that they will comply with certain obligations. The CFPB concludes that this certification-based approach is the appropriate approach for ensuring that third parties are acting on behalf of consumers when they are accessing covered data. Some commenters had urged the CFPB to impose obligations directly on third parties, including data aggregators, and to supervise third parties, including data aggregators, to ensure compliance. They raised concerns about how the obligations could be enforced under a certification-based approach if the authorized third party or data aggregator fails to comply with their obligations. The CFPB has concluded that these obligations can be enforced effectively under the certification-based approach in various ways, including by the CFPB using its authority to prevent unfair, deceptive, or abusive acts or practices; by other regulators; and potentially by consumers under other applicable statutes or common law. With respect to supervision of third parties, as discussed in part IV.5, the CFPB's supervisory authority is defined by the CFPA. The CFPB will continue to monitor the market, including by using its supervisory authority, and will consider whether additional rulemakings are appropriate to expand the scope of the CFPB's supervision with respect to part 1033.

The CFPB declines to include in the final rule additional protections requested by commenters. The authorization procedures provide significant protections for consumers to

ensure that third parties accessing covered data are acting on behalf of the consumers. The CFPB has concluded that it is unnecessary to include in the rule specific prohibitions on false or misleading representations or omissions to induce consumers to consent to third party access to covered data. Other provisions of law, including the protections of the CFPA against unfair, deceptive, or abusive acts or practices, already would address such conduct. The CFPB also declines to impose a waiting period before a third party can solicit additional authorizations. The limitation on a consumer's requested product or service is intended to be flexible for consumers to determine for themselves if they want multiple products or services, which they can authorize separately through the authorization procedures. The CFPB also notes that the rule includes a clear limitation that third parties must not expand collection, use, or retention of covered data beyond the scope of the product or service described in the consumer's authorization.

To avoid being overly prescriptive, and in light of CFPA section 1033(e)'s objective of technological neutrality, the final rule does not specify methods or mechanisms that third parties must use to obtain express informed consent electronically. Regardless of the method or mechanism used, the third party must obtain a written or electronic signature that the consumer executes or adopts with the intent to sign the authorization disclosure. When determining the method or mechanism that it will use to obtain an authorization disclosure signed in writing or electronically by the consumer, a third party must consider all of the final rule's provisions related to the authorization disclosure as well as the CFPA's prohibition on unfair, deceptive, or abusive acts or practices and other applicable law. For example, under final § 1033.411(a), the third party must provide the authorization disclosure electronically or in writing. Under final § 1033.421(g), a third party must certify that it will provide a consumer with a copy of the authorization disclosure that has been signed by the consumer electronically or in writing and

that reflects the date of the consumer's electronic or written signature. Certain third parties also must establish and maintain written policies and procedures that are reasonably designed to ensure retention of records that are evidence of compliance with the requirements of subpart D. A third party may not be able to satisfy these requirements if it obtains a consumer's electronic signature by certain methods or mechanisms. For example, the CFPB expects that in order to ensure accuracy, record integrity, and to preserve the ability to access the signed authorization disclosure, the authorization disclosure and the electronic signature establishing consumer consent cannot as a matter of regular course be provided orally and still satisfy all of the final rule's requirements.[90]

The final rule has adopted the proposed approach to authorization by joint account holders. As provided in § 1033.331(d), a data provider that receives a request for a covered data from a consumer that jointly holds an account or from an authorized third party acting on behalf of that consumer must provide covered data to that consumer or authorized third party. When a third party is seeking covered data on behalf of a consumer that jointly holds an account, the third party must comply with the authorization procedures for the joint account holder on whose behalf the third party is requesting access. Consistent with the discussion in part IV.C.5 in connection with § 1033.331(d), an authorization from a single account holder is sufficient for an authorized third party to access covered data, and the CFPB declines to require that other joint account holders be notified or receive copies of the authorization disclosure.

Finally, the CFPB declines to establish any exceptions to the authorization procedures for certain third parties, such as smaller third parties or non-commercial third parties. The CFPB has

[90] Programs, goods, and services provided to the general public must be accessible to consumers with disabilities. Third parties should ensure that their authorization and consent procedures enable, when appropriate, the use of assistive technologies that may be warranted under the ADA or other applicable law.

concluded that it would be difficult to define the appropriate scope of any such exceptions at this time and is concerned that such exceptions could create loopholes. The CFPB has designed the authorization procedures so that they should not be overly difficult for third parties to navigate. Moreover, the rule does not prohibit persons such as attorneys or accountants from making arrangements for the consumer to provide financial information, included covered data.

3. Authorization disclosure (§ 1033.411)

Proposed § 1033.411 specified format and content requirements for the authorization disclosure that third parties would provide to consumers in order to be authorized to access covered data on behalf of the consumer, as set forth in proposed § 1033.401. As discussed below, the final rule maintains format and content requirements for the authorization disclosure with several adjustments.

General requirements (§ 1033.411(a))

Proposed § 1033.411(a) would have required that, to comply with proposed § 1033.401(a), a third party must provide the consumer with an authorization disclosure electronically or in writing. It also would have set forth general format requirements for the authorization disclosure. Specifically, the CFPB proposed that the authorization disclosure must be clear, conspicuous, and segregated from other material. The CFPB preliminarily determined that these requirements would facilitate consumer understanding of the authorization disclosure. The CFPB also preliminarily determined that requiring the authorization disclosure to appear segregated from other material would help ensure consumers read and understand the authorization disclosure by avoiding overwhelming consumers with extraneous information and diluting the informational value of the authorization disclosure.

The CFPB sought comment on whether these formatting requirements would aid consumer understanding and whether additional requirements should be included in the rule. Specifically, the CFPB sought comment on whether the rule should contain more prescriptive requirements, such as specifying a word count or setting a reading level. The CFPB also sought comment on whether the rule should include a timing requirement, such as a requirement that the authorization disclosure be provided close in time to when the third party would need consumer data to provide the product or service. Additionally, the CFPB sought comment on whether indicia that the authorization disclosure is clear, conspicuous, and segregated from other material should include utilizing a format or sample form that is set forth in a qualified industry standard.

As stated in the proposed rule, the CFPB considered proposing specific guidance for accessibility of the authorization disclosure for individuals with disabilities but preliminarily determined that the Americans with Disabilities Act (ADA) and its implementing regulations[91] would already require that the authorization disclosure be provided in an accessible format. The CFPB sought comment on whether the rule should contain requirements relating to the accessibility of the authorization disclosure.

The CFPB received a number of comments on the authorization disclosure's general requirements. A variety of commenters, including data providers and trade associations for certain data providers, some third parties and trade associations for certain third parties, and a research institute, supported the proposed formatting requirements because the commenters thought that the proposed requirements are clear, straightforward, and meaningful. A commenter suggested that the proposed provisions related to written authorization disclosures should be removed because they are unnecessary.

[91] *See* 42 U.S.C. 12132, 12182(a); 28 CFR 35.130, 35.160(a), 36.201, 36.303(c).

A variety of commenters, including data providers and trade associations for certain data providers, some third parties, consumer advocates, and a research institute, supported adding various requirements for the authorization disclosure, including plain language, reading level, or understandability requirements. One consumer advocate commenter supported a word count limit for consumer understandability, but a research institute commenter opposed a word count limit. This commenter said that a word count limit would not be feasible based on the amount of information that may need to be included in the authorization disclosure.

A consumer advocate commenter and two data provider commenters supported adding authorization disclosure timing requirements to the rule. The consumer advocate commenter suggested that the rule specify that the authorization disclosure be provided no earlier than 14 days prior to the time that the third party begins providing the product or service to the consumer. One of the data provider commenters suggested that the authorization disclosure should be provided close in time to when the third party would need covered data to provide a product or service, and the other data provider commenter similarly suggested that the authorization disclosure be provided close in time to when the third party first accesses covered data. The consumer advocate commenter and two data provider commenters suggested that timing standards could increase the chances that a consumer is making an informed choice to authorize a third party to access covered data and reduce the risk that a consumer forgets that they previously authorized a third party to access covered data.

A variety of commenters, including data providers, third parties, a consumer advocate, and a research institute, suggested adding other formatting requirements to increase consumer understanding. Some data providers, trade associations for certain data providers, and a third party commenter requested additional clarity on the meaning of "clear and conspicuous." A trade

association for data providers requested that the final rule prohibit extraneous language that could cause consumer confusion or obscure key terms of access. One third party commenter expressed concern that the proposed requirement to segregate the disclosure from other material would cause consumers to over-focus on the authorization disclosure. This commenter supported allowing the authorization disclosure to be combined with other materials, including disclosures required under Regulation E or Regulation Z. However, several commenters supported requiring that the authorization disclosure be segregated from other material.

A standard-setting organization commenter asserted that the use of qualified industry standards regarding the authorization disclosure would not be appropriate for establishing regulatory compliance or as indicia of compliance, but stated that specifications and best practices might evolve to match the final rule and be used as suggestive tools. Some trade association commenters and a credit union commenter supported a role for industry standards in authorization disclosure formatting because, they said, it would improve consistency in the disclosures. A third party commenter stated that when consumers have multiple accounts, the rule should ensure that consumers check a box or similarly identify the accounts to which consumers are granting access, noting that this requirement could be defined by industry standards.

Commenters also provided feedback on whether the CFPB should provide model forms for the authorization disclosure in addition to setting forth general formatting requirements in the rule. A variety of commenters, including data providers, consumer advocates, and a research institute, suggested that the CFPB provide model forms or clauses for all or part of the authorization disclosure to save time and resources and ensure effectiveness, consistency, and compliance. Two consumer advocate commenters and a bank commenter suggested that model

forms would be beneficial for consumers. A bank trade association commenter and a data aggregator commenter suggested that use of model forms should provide a safe harbor. Conversely, one trade association commenter specifically opposed model forms. This commenter opposed over-engineered and overly prescriptive requirements for the authorization disclosure. One third party commenter preferred flexible standards that would allow authorization disclosures to shift with market innovations and new technologies.

A consumer advocate commenter requested a disability accessibility requirement to prevent any ambiguity in case there is a disagreement about the applicability of the ADA.

For the reasons discussed herein, the CFPB is finalizing the language of § 1033.411(a) as proposed, with an additional requirement. Specifically, the CFPB is adding to final § 1033.411(a) a requirement that the names included in the authorization disclosure, as required by §§1033.411(b)(1) and (2) and by § 1033.431(b), must be readily understandable to the consumer. The CFPB has determined that this requirement will help ensure that consumers are able to easily identify the entities in the authorization disclosure. Unlike a legal or trade name which may or may not be familiar to a consumer depending on the particular entity, the "readily understandable" requirement directly addresses consumer understanding to facilitate informed consent.

The CFPB is not eliminating the option for third parties to provide the authorization disclosure in writing as suggested by a commenter. Retaining this option permits flexibility in circumstances that may necessitate the authorization disclosure to be provided in a non-electronic form.

The CFPB is not including the additional formatting requirements requested by commenters, including plain language or reading level requirements or word count limits,

because "clear and conspicuous" is a common standard that is flexible enough to cover a variety of circumstances and ensure consumer understanding of the authorization disclosure. The meaning of "clear and conspicuous" in this final rule should be informed by how the standard has been interpreted in other contexts, including by the FTC in assessing whether disclosures in advertisements are clear and conspicuous.[92]

The CFPB is not including timing requirements, as suggested by some commenters, in order to maintain flexibility in light of the variety of products and services for which third parties may seek to access covered data. For example, a third party may need to access covered data periodically, may only need to access covered data at or near the time that the consumer obtains the product or service, or may only need to access covered data at a later time. Additionally, the final rule's duration and reauthorization requirements act as added protections against potential harms related to third parties accessing covered data based on long-term authorizations.

The CFPB is maintaining the proposed segregation requirement for the authorization disclosure. Combining disclosures or other materials that serve varying purposes in the manner that a third party commenter suggested could result in consumer confusion. Although Regulation E and Regulation Z disclosures provide important consumer protections, they do not serve the same purposes as the authorization disclosure, which is to ensure that third parties are acting on behalf of consumers when accessing covered data. Simply placing the authorization disclosure at the top of a combined disclosure form would not sufficiently alleviate the risk of consumer confusion. Moreover, segregating the authorization disclosure from other material,

[92] The FTC has articulated the "4 Ps"—prominence, presentation, placement, and proximity—as a way of evaluating whether disclosures are clear and conspicuous. Lesley Fair, *Full Disclosure*, FTC Bus. Blog (Sept. 23, 2014), https://www.ftc.gov/business-guidance/blog/2014/09/full-disclosure.

including other important disclosures, allows the consumer to consider the content of each disclosure or other document in turn.

The CFPB is not providing model forms or clauses for the authorization disclosure. The final rule provides flexibility in how third parties meet the disclosure requirements given the range of potential third parties that may seek authorization to access covered data pursuant to the final rule's framework and the potential for innovation and the development of new technologies. As one research institute commenter noted when discussing a word count limit, there may be feasibility issues with providing a model disclosure because it potentially would need to be useable for multiple different types of products and services, multiple data providers, and multiple third parties. The CFPB will monitor the market and consider developing model forms or clauses in the future, as appropriate.

The final rule does not reference a consensus standard regarding authorization disclosure format because the clear and conspicuous standard is well established in Federal consumer financial law, as well as other consumer protection frameworks in both State and Federal law. Additionally, the CFPB encourages third parties and other interested stakeholders to apply to test authorization disclosures through the CFPB's Trial Disclosure Policy.[93]

The CFPB is not including disability accessibility requirements in the final rule because the ADA addresses these requirements, and the CFPB does not want to create potentially conflicting requirements.

[93] Consumer Fin. Prot. Bureau, *Competition and innovation at CFPB*, https://www.consumerfinance.gov/rules-policy/competition-innovation/ (last visited Oct. 16, 2024). Under this policy, companies can obtain a safe harbor for testing disclosures that improve upon existing disclosures for a limited period of time while sharing data with the CFPB.

Authorization disclosure content (§ 1033.411(b))

Proposed § 1033.411(b) would have required inclusion of the following key terms of access in the authorization disclosure: (1) the name of the third party that will be authorized to access covered data pursuant to the third party authorization procedures in proposed § 1033.401; (2) the name of the data provider that controls or possesses the covered data that the third party seeks to access on the consumer's behalf; (3) a brief description of the product or service that the consumer has requested the third party provide and a statement that the third party will collect, use, and retain the consumer's data only for the purpose of providing that product or service to the consumer; (4) the categories of covered data that will be accessed; (5) the certification statement described in proposed § 1033.401(b); and (6) a description of the revocation mechanism described in proposed § 1033.421(h)(1). Additionally, proposed § 1033.431(b) would have required the authorization disclosure to include the name of any data aggregator that would assist the third party with accessing covered data and a brief description of the services the data aggregator would provide.

The proposed content requirements for the authorization disclosure aimed to strike a balance between providing consumers with sufficient information to enable informed consent to data access and keeping the disclosure sufficiently short to increase the likelihood that consumers will read and understand it. The CFPB preliminarily concluded that the proposed requirements would be important for consumers to understand the terms of data access and would help ensure that third parties accessing covered data are acting on behalf of consumers by enabling informed consent.

The CFPB sought comment on any obstacles to including the proposed authorization disclosure content and on whether additional content was needed to ensure consumers have

enough information to provide informed consent. Specifically, the CFPB sought comment on whether the rule should include any additional requirements to ensure: (1) the consumer can identify the third party and data aggregator, such as by requiring inclusion of legal names, trade names, or both; (2) the description of the consumer's requested product or service is narrowly tailored and specific such that it accurately describes the particular product or service that the consumer has requested; (3) the consumer can locate the third party obligations, such as by requiring a link to the text of proposed § 1033.421; and (4) the consumer can readily understand what types of data will be accessed, such as by requiring third parties to refer to the covered data they will access using the categories in proposed § 1033.211. The CFPB also sought comment on whether the authorization disclosure should include additional content such as the names of other parties with whom data may be shared, the third party's contact information, or how frequently data will be collected from the consumer's account(s).

A variety of commenters supported the authorization disclosure content included in the proposed rule on the grounds that it would provide consumers with information that would enable informed consent. A variety of commenters also stressed the importance of keeping the authorization disclosure short to avoid information overload for consumers. One research institute commenter requested harmonization of the authorization disclosure with other privacy laws to reduce compliance challenges and consumer confusion.

A variety of commenters suggested that additional content be included in the authorization disclosure.[94] A bank, bank trade association, and a consumer advocate also

[94] One or more commenters requested that one or more of the following be included in the authorization disclosure: the legal and trade name of the third party; a description of the data security and privacy standards to which the third party will adhere in relation to the consumer's data; contact information for the third party, aggregator, and/or the CFPB; a link to the third party's website; information about the frequency (how often data are accessed), recurrence (such as one time data access or recurring access), and duration of data access or retention (time period when data

recommended that additional content be included through a hyperlink on the authorization disclosure.

Other commenters, including a data aggregator, a trade association for certain third parties, a data provider, a consumer advocate, and a research institute, suggested that the content should be limited. Two of these commenters expressed concern about information overload, and two commenters expressed concern about the burden of including additional information in the authorization disclosure. A data provider commenter requested that the final rule remove the requirement to include the data provider's name in the authorization disclosure.

Some commenters, including a credit union commenter, trade association commenters, and a consumer advocate commenter, supported additional requirements to ensure the description of the consumer's requested product or service is narrowly tailored and specific. One data aggregator commenter requested clarification on the description needed to identify the categories of data that will be accessed. This commenter suggested that it should be sufficient to use categories such as "transactional history" or "account balance" and that it should not be necessary to describe more specific data fields.

For the reasons discussed herein, the CFPB is finalizing § 1033.411(b) with modifications. First, the final rule adds a requirement, as § 1033.411(b)(6), that the authorization disclosure include a brief description of the expected duration of data collection and a statement that collection will not last longer than one year after the consumer's most recent reauthorization. The content of proposed § 1033.411(b)(6) is finalized as § 1033.411(b)(7). Second, the final rule

---

are accessed or retained); a description of any alternatives to sharing covered data that would allow a consumer to access the product or service (for example, providing a credit score for credit underwriting or microtransfers to the consumer's bank account to verify the account); the names of other third parties with whom data may be shared; a brief explanation of the ways in which data that identifies the consumer can be used by the third party accessing the data; and the specific purposes for which the third party collects and uses the consumer's data.

removes the word "covered" from § 1033.411(b)(4) and specifies that the disclosure for categories of data that will be accessed must have a substantially similar level of specificity as the categories in § 1033.211. The other modifications are non-substantive adjustments for clarity and consistency.

The CFPB is finalizing in § 1033.411(b)(6) a requirement that third parties include a description of the expected duration of data access because this requirement is important for consumers to understand the terms of data access. In particular, including information about the revocation method in the authorization disclosure without information about the duration of collection could leave consumers under the mistaken impression that the only way for data access to end is through utilizing the revocation method. Duration is also a key term that may help consumers decide whether to consent to third party data access. In the case of a one-time data pull, this additional information lets consumers know the data sharing will not continue. In the case of authorizing data access without a set duration, this additional information ensures consumers know about the one-year reauthorization requirement.

By removing the word "covered" from § 1033.411(b)(4), the final rule allows the authorization disclosure to include categories of non-covered data. This gives third parties the flexibility to utilize the authorization procedures to access non-covered data in addition to covered data. The additional requirement that the categories used in the authorization disclosure must have a substantially similar level of specificity as the categories in § 1033.211 will help ensure that consumers have enough information about what types of data are being accessed while also ensuring that the authorization disclosure does not become too lengthy due to a long list of very specific data types.

Beyond these modifications, the CFPB is not adding or eliminating content requirements for the authorization disclosure in the final rule, as requested by some commenters. The content requirements strike an appropriate balance between providing consumers with sufficient information to enable informed consent to data access and keeping the disclosure sufficiently short to increase the likelihood that consumers will read and understand it. Regarding the commenter suggesting clarification on the description of the categories of data to be accessed, the CFPB notes that the categories of data that will be accessed must have a substantially similar level of specificity as the categories in § 1033.211. Finally, the CFPB has determined that third parties can comply with the authorization disclosure content requirements in § 1033.411(b) while also complying with other applicable privacy laws.

Language access (§ 1033.411(c))

Proposed § 1033.411(c)(1) would have required that the authorization disclosure be provided in the same language as the communication in which the third party conveys the authorization disclosure to the consumer. It also would have required any translation of the authorization disclosure to be complete and accurate. Proposed § 1033.411(c)(2) stated that if the authorization disclosure is in a language other than English, it must include a link to an English-language translation. Additionally, proposed § 1033.411(c)(2) stated that, if the authorization disclosure is in English, it would be permitted to include links to translations in other languages.

The proposed rule stated that consumers with limited English proficiency may benefit from receiving a complete and accurate translation of the authorization disclosure, and some third parties may want to respond to the needs of consumers with limited English proficiency using translated disclosures. At the same time, the CFPB preliminarily determined that requiring

third parties to identify such consumers and provide complete and accurate translations in the myriad languages that consumers speak may impose a significant burden on third parties.

The proposed rule stated that some consumers who receive translated disclosures may also want to receive English-language disclosures, either because they are fluent in English, or because they wish to share the disclosures with an English-speaking family member or assistance provider. It also stated that English-language disclosures may also allow consumers to confirm the accuracy of the translation.

The CFPB received few comments on the proposed language access provisions. One trade association for nondepositories indicated that the language access provision is satisfactory. A consumer advocate commenter requested that the CFPB require the authorization disclosure to be translated into languages used in marketing. Another consumer advocate commenter requested a Spanish language disclosure and stated that the rule should require third parties to automatically provide the authorization disclosure and other documents in Spanish to all consumers. This commenter also suggested that the rule improve language access throughout the entirety of the data gathering process and hold data aggregators and lenders to comparable standards. A bank trade association commenter suggested that the language access provision in the proposed rule necessitated additional discussion or clarity regarding how principles regarding unfair, deceptive, or abusive acts or practices apply more generally to financial products and services on an end-to-end basis.

For the reasons discussed herein, the CFPB is finalizing the language access provisions in § 1033.411(c) as proposed, with nonsubstantive clarifying changes. The final rule's language access requirement applies to the authorization disclosure and, where applicable, the data aggregator certification. The language access provisions in the final rule ensure that a consumer

understands and is able to exercise control over what covered data the third party would collect, use, and retain. The CFPB has determined that it would not be appropriate to require authorization disclosures to be provided to all consumers in Spanish, as requested by one commenter. The requirement in § 1033.411(c)(1) to provide the authorization disclosure in the same language as the communication in which the authorization disclosure is conveyed to the consumer should help ensure that consumers receive the disclosure in a language they understand, without a broad requirement that all authorization disclosures be provided in Spanish, which would result in additional burden on third parties. A broad statement about the interaction of principles regarding unfair, deceptive, or abusive acts or practices and language access more generally is outside the scope of this rulemaking.

4. Third party obligations (§ 1033.421)

Proposed § 1033.421 described obligations to which third parties would be required to certify in order to be authorized to access covered data. The proposed third party obligations included: a limit on third party collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service; a maximum duration of collection of one year after the consumer's most recent authorization unless the consumer provides a new authorization; and certifications that the third party would provide consumers a simple way to revoke access, maintain certain accuracy and data security obligations, and ensure consumers have access to information about the third party's authorization to access data. The CFPB stated that it was proposing these certification requirements to ensure that third parties accessing covered data are acting on behalf of the consumer.

The proposed third party obligations received a range of feedback from commenters, with some commenters offering general support for the proposed approach to requiring third parties to certify to the obligations in proposed § 1033.421, while other commenters expressed concern with the proposed obligations and the associated privacy protections.[95] Some commenters suggested that aspects of the proposed obligations do not accord with congressional intent to ensure consumers can use their own data for their own preferences, and that the CFPB lacks authority to prescribe the proposed obligations. Other commenters said the obligations are not strong enough to protect consumers' privacy. Specific comments are discussed in more detail in the sections regarding third party obligations, below.

The CFPB is prescribing the third party obligations in § 1033.421 to ensure that third parties accessing covered data are acting on behalf of consumers, consistent with CFPA section 1033. As explained above in the legal authority discussion in part IV.D.1, the plain language of CFPA section 1033(a) provides that, subject to rules prescribed by the CFPB, a covered person shall make available to a "consumer," upon request, certain information in the control or possession of the covered person. CFPA section 1002(4) defines "consumer" as "an individual or an agent, trustee, or representative acting on behalf of an individual." For convenience, part 1033 generally refers to the individual as the "consumer" and an agent, trustee, or representative acting on behalf of that individual as an "authorized third party." Congress intended, through CFPA section 1033, that the consumer would have the right to access their covered data for their own benefit, and would be able to authorize representatives to act on their behalf to that end. As such, the final rule requires third parties accessing covered data to adhere to the procedures and

[95] A research institute commenter stated that the final rule should clarify that data generated by a third party in the course of providing the consumer's requested product or service is not subject to the third party obligations. Use of generated data is discussed below related to § 1033.421(c).

obligations in subpart D, including certifying to limit collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service, so as to ensure that the third party is accessing data as a representative acting on behalf of the consumer and that the consumer is the primary beneficiary of that data access. In addition, as noted above, the CFPB has rulemaking authority to adopt § 1033.421 to carry out the objectives of CFPA section 1033.

By adhering to the obligations in § 1033.421, a third party, as a representative acting on behalf of the consumer, ensures consumers are best positioned to understand the data access they are authorizing and accordingly are best positioned to exercise meaningful control with respect to such access. As such, the obligations in § 1033.421 ensure the consumer is effectively informed about the scope of the third party's access to covered data and ensure that the third party's access accords with the intent and reasonable expectations of the consumer. For example, the third party's adherence to § 1033.421(a) ensures the consumer understands and clearly directs how and for what purposes their data will be collected, used, and retained.

For the reasons discussed herein, final § 1033.421 generally adopts the proposed third party obligations. Changes related to specific aspects of the proposed obligations are described in detail below.

General standard to limit collection, use, and retention (§ 1033.421(a))

Under proposed § 1033.421(a)(1), third parties would have been required to limit collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service. Proposed § 1033.421(a)(2) would have provided that, for purposes of the limitation in proposed § 1033.421(a)(1), certain listed activities would not be part of, or reasonably necessary to provide, any other product or service. Under these proposed

provisions, third parties would seek and obtain consumer authorization to access covered data only as reasonably necessary for the provision of the product or service that the consumer requested, and not for uses that are secondary to that purpose.

The proposed rule explained that the limit on collection, use, and retention of covered data in § 1033.421(a) was designed to ensure that, consistent with carrying out the objectives of CFPA section 1033, third parties that access covered data would act on behalf of consumers, and that third party collection, use, and retention of covered data would proceed in alignment with consumer control and truly informed consent. Specifically, proposed § 1033.421(a) was aimed at ensuring that third parties access covered data for the consumer's benefit, that consumers retain meaningful control over their data when authorizing third party access to that data, and that consumers are best positioned to understand the scope of that authorization. In addition, proposed § 1033.421(a) was aimed at ensuring consumers do not unknowingly or reluctantly acquiesce to data collection, use, and retention that they do not want. Further, the proposed rule noted that covered data that third parties would collect, use, and retain pursuant to consumer authorization would include sensitive financial data that might subject consumers to fraud or identity theft if it were exposed.[96] The proposed rule stated that the limitation in § 1033.421(a) was designed to ensure that third parties would act on behalf of consumers when accessing that sensitive data.

The CFPB is generally finalizing § 1033.421(a) as proposed. Feedback from commenters, and the CFPB's approach in the final rule, are discussed further below related to each aspect of the general data limitation standard.

[96] These sensitive data also could impact persons or entities besides the consumer from whom they are sourced, especially when collected, used, and retained in large amounts, such as where the data are matched with other consumer data sets.

In general (§ 1033.421(a)(1))

The CFPB is finalizing § 1033.421(a)(1) as proposed. Under final § 1033.421(a)(1), third parties must certify to limit collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service. Specific aspects of the standard in § 1033.421(a)(1), including comments received and rationale for the final provisions, are discussed below.

Reasonably necessary

As described in the proposed rule, the reasonably necessary standard was designed to ensure that the consumer is the primary beneficiary of any authorized data access, and that the resulting collection, use, and retention of covered data align with consumer control and informed consent. The CFPB considered a range of alternatives to this standard, including evaluating limitation standards in other data privacy regimes.[97] For example, the CFPB considered whether data collection, use, and retention should be limited to what is "strictly necessary," "adequate," "relevant," or "legitimate." The CFPB preliminarily determined that a reasonably necessary standard would be flexible enough that third parties could use data for a variety of purposes to provide the product or service the consumer requested, but would still sufficiently minimize third party collection, use, and retention to ensure third parties accessing covered data are acting on behalf of the consumer.

The reasonably necessary standard received general support from many commenters, including data providers, consumer advocates, third parties, data aggregators, Members of

[97] The proposed rule stated that the reasonably necessary standard in proposed § 1033.421(a)(1) would be similar to standards in several data privacy frameworks that minimize third parties' collection, use, and retention of data. *See, e.g.*, *Competition and Consumer (Consumer Data Right) Rules 2020*, div. 1.3 (Austl.) (minimizing consumer data requests to what is "reasonably needed"); Reg. 2016/679, art. 5(1)(c), 2016 O.J. (L 119) 7 (EU) ("Personal data shall be . . . limited to what is necessary in relation to the purposes for which they are processed.").

Congress, trade associations for data providers, and others. These commenters expressed support for third parties generally limiting their collection, use, and retention of data based on what is reasonably necessary. Some commenters who supported the reasonably necessary standard offered for consideration various clarifications or feedback on other aspects of the rule, like how the standard might apply to collection, use, or retention separately. These comments are discussed below related to those provisions.

Some commenters—mostly third parties and related trade associations, but also some banks, trade associations for data providers, and consumer advocates—expressed concerns about the proposed reasonably necessary standard. Some of these commenters posited that the proposed standard is stricter than other privacy regimes, might result in unintended consequences for consumers, does not give consumers meaningful control, or would result in an unlevel playing field between data providers and third parties. Other commenters suggested that the reasonably necessary standard does not go far enough to constrain downstream data uses not requested by consumers or to curb activities by data aggregators that would not be necessary for the provision of the product or service. Other commenters suggested alternative standards, either from industry or from other privacy laws, regulations, and principles. Some commenters suggested that collection, use, and retention each should be governed by different standards. In contrast, some third party commenters stated that the reasonably necessary standard for collection is too rigid and impractical for some products and services. Comments related to the application of the general limitation standard to collection, use, and retention are discussed separately below in more detail.

For the reasons discussed herein, the CFPB is finalizing the reasonably necessary standard in § 1033.421(a) as proposed. The CFPB considered whether a stricter standard should apply to more sensitive types of data, and generally whether other standards would be more

consumer protective. After considering comments received and the CFPB's evaluation of alternatives, the CFPB has determined that the reasonably necessary standard is sufficiently flexible for third parties to collect, use, and retain covered data for a variety of purposes to provide the product or service the consumer requested, but will still sufficiently minimize third party collection, use, and retention to ensure third parties accessing covered data are acting on behalf of the consumer. The CFPB disagrees with commenters that suggested the standard is too rigid or impractical, or too permissive for third parties such that it would not protect consumers from downstream uses or result in other unintended consequences. The reasonably necessary standard will protect consumers from unwanted data collection, use, and retention while giving third parties sufficient flexibility to collect, use, and retain data to provide consumers the products or services they request. As such, the CFPB declines to make commenters' suggested changes to the proposed standard.

As described further below, the CFPB has determined that collection, use, and retention of covered data beyond what is reasonably necessary for the product or service the consumer requested would undermine the consumer's understanding of the authorizations they provided and would thus undermine a consumer's ability to control their data. The third party obligations, including the limit on collection, use, and retention of covered data, are designed to ensure that the third party is accessing covered data for the consumer and that accordingly the consumer is the primary beneficiary of that data access. Third parties can benefit from access to covered data, but only by collecting, using, and retaining data as reasonably necessary to provide the consumer's requested product or service.[98] A third party that collects, uses, or retains data in a

[98] Consumers benefit by authorizing third parties to collect, use, or retain their data for the product or service they request, and from having confidence third parties will not do so other purposes. The third party's obligations to the consumer do not prevent the third party from benefiting from access to covered data. As noted above, third parties

manner that benefits the third party but that is not reasonably necessary for the product or service the consumer requested would not be acting on behalf of the consumer. In that situation, the third party would be advancing their own the interests, and not the interests of the consumer, and as such would not be acting as a representative acting on behalf of the consumer within the meaning of CFPA section 1002(4).

Consumer's requested product or service

Under proposed § 1033.421(a)(1), third parties would have been required to limit collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service. The second aspect of this standard, "the consumer's requested product or service," was designed to carry out the objectives of CFPA section 1033. The proposed rule explained that consumers generally go into the market seeking the core function of a product or service and, when authorizing data access, intend for their data to be accessed for that purpose. The proposed rule explained further that third parties can significantly benefit from accessing consumers' covered data, and consumers often do not know about various data uses, do not want companies to use their data broadly, and also generally lack bargaining power to adequately protect their data privacy. The proposed rule stated that, as a result of this imbalance, third parties often broadly collect, use, and retain covered data for their own benefit. The CFPB preliminarily determined that the proposed standard being grounded in the "consumer's requested product or service" would ensure third parties only collect, use, and retain covered data on consumers' behalf, pursuant to informed consent.

---

can benefit from such access by collecting, using, and retaining data as reasonably necessary to provide the consumer's requested product or service. In other words, the way a third party can benefit is through the opportunity to provide the consumer the product or service that they are requesting.

To avoid circumvention of this standard, the CFPB proposed to treat the product or service as the core function that the consumer sought in the market and that accrues to the consumer's benefit. The preamble to the proposed rule explained that the scope of the product or service would not be defined by disclosures, and the CFPB noted its concern that disclosures could be used to create technical loopholes by expanding the scope of the product or service the consumer requested to include any activity the company would choose, including those that would benefit the third party, not the consumer. As such, proposed § 1033.421(a)(1) was intended to help ensure that third parties act for the benefit of consumers, that consumers retain control over their authorizations for data access, and that consumers are best positioned to provide meaningfully informed consent to third party collection, use, and retention of their covered data.

Some commenters requested clarifications or suggested that the proposed general standard should be changed with respect to its approach to the consumer's requested product or service. A data aggregator commenter stated that the final rule should rely on "reasonably necessary" only, and should not limit collection, use, or retention by the consumer's requested product or service. This commenter stated that this change would allow third parties to use previously collected data as reasonably necessary to provide additional products or services the consumer requests at a later time. Other commenters requested clarifications about the proposal's approach to the consumer's requested product or service. For example, a trade association for data providers, a data provider, and a third party requested that the phrase "consumer's requested product or service" be defined or clarified. A trade association for data providers further stated that the description of the consumer's requested product or service in the preamble to the proposed rule gave the impression that the CFPB intended to decide on a case-by-case basis,

based on specific consumer understanding, what the scope of a requested product or service is and then determine whether data access based on that scope was reasonably necessary. A third party stated that the scope of a consumer's requested product or service would be unclear in light of how products or services are currently offered to consumers in the market, as the preamble to the proposed rule potentially would have divided a product or service by its core functions or component parts.

For the reasons discussed herein, the CFPB is finalizing § 1033.421(a) as proposed. Under final § 1033.421(a), a third party's collection, use, and retention of covered data must be reasonably necessary to provide the "consumer's requested product or service." By limiting third party collection, use, and retention of covered data based on "the consumer's requested product of service," the final rule ensures that such collection, use, and retention is for the consumer's benefit, that consumers retain control over their authorizations for data access, and that consumers are best positioned to providing meaningfully informed consent to third party collection, use, and retention of covered data. As such, the CFPB declines to adopt commenters' suggestions to finalize the general limitation standard without reference to the "consumer's requested product or service," or to otherwise expand the general limitation standard in ways that would allow for covered data to be used for additional products or services or other purposes.

To address commenters' concerns about potential confusion, the CFPB notes that "the consumer's requested product or service" in § 1033.421(a) is not intended to result in a case-by-case inquiry into a specific consumer's understanding of the requested product or service. Rather, what constitutes a consumer's requested product or service is informed by context, such as general public understanding of what attributes a given product or service has or how the product or service functions in the market. The third party cannot rely on disclosures to expand

the scope of a consumer's requested product or service or use disclosures to create technical loopholes and include any purposes the company chooses. The CFPB notes that, in the course of seeking authorization to access covered data, some third parties might attempt to expand the scope of products or services offered to consumers in an effort to access covered data for purposes that do not primarily benefit consumers. Along those same lines, some third parties might purport to offer a product or service to a consumer that is merely a pretext for collecting, using, and retaining covered data from the consumer.[99] Where third parties seek to use data to advance their own interests, rather than to act for the consumer, such actions would not be on behalf of the consumer, and thus would not be in accordance with the text of sections 1002 and 1033 of the CFPA.

Additionally, the CFPB notes that the discussion in the proposal's preamble related to the product or service's core function was not intended to suggest that each product or service would necessarily have only a single attribute. As described above, if a consumer requests a product or service with a commonly understood set of attributes, the third party cannot expand the scope of the product or service for purposes of § 1033.421(a) by including in its disclosures to consumers attributes that are not consistent with the general public understanding of that product or service or how that product or service functions in the market. Whether attributes are associated with a product or service could be indicated if those attributes are widely available as, or generally compose, those products or services. While a third party might offer to a consumer, even within a single mobile application, two products or services for which a consumer might authorize data access, like a budgeting service and a payments service, these services are sufficiently different

[99] The CFPB notes that such a practice would be inconsistent with § 1033.401, which provides that third parties must seek access to covered data on behalf of the consumer to provide a product or service the consumer requested.

as to necessitate two separate authorizations for the purposes of § 1033.421(a). Similarly, while a credit card and a prepaid card share many attributes, they are, and are commonly understood to be, different types of products. Accordingly, authorization for data access to provide a credit card would not be sufficient authorization for data access to provide a prepaid card.

Specific purposes (§ 1033.421(a)(2))

Proposed rule

In addition to the general limitation on collection, use, and retention of covered data in § 1033.421(a)(1), proposed § 1033.421(a)(2) stated that targeted advertising, cross-selling of other products or services, or the sale of covered data would not be part of, or reasonably necessary to provide, any other product or service. Relying on stakeholder feedback and research, the proposed rule described that third parties generally do not include these activities in products or services for consumers' benefit, but instead do so for their own benefit.[100] These activities are pervasive in the market, consumers often lack choices about whether their data can be used for these purposes, and consumers often do not expect their data to be used for them. In addition, the CFPB stated that consumers often do not understand these activities' potential for harm, while also noting that third parties can greatly benefit from these activities. For all these reasons, the CFPB preliminarily determined that when a third party combines targeted advertising, cross-selling, and data sales with any other consumer requested products or services, it is generally doing so for its own benefit, and that such combination would interfere with

[100] *See, e.g.*, Rodney John Garratt & Michael Junho Lee, *Monetizing Privacy*, at 4, Fed. Rsrv. Bank of N.Y. Staff Rep. No. 958 (Jan. 2021), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr958.pdf ("Most of the gains from consumer data do not go to consumers."); Raheel A. Chaudhry & Paul D. Berger, *Ethics in Data Collection and Advertising*, 2 GPH Int'l J. of Bus. Mgmt. 1, 5-6 (2019), http://www.gphjournal.org/index.php/bm/article/view/240/110 (stating that targeted advertising and data monetization allow companies to collect, use, and retain "consumer data without the user being any the wiser," and that targeted advertising and data monetization elevate "the risk involved in data breaches and malicious parties buying consumer data on the secondary data market").

consumer control and understanding. The CFPB also preliminarily determined that it would not be consistent with carrying out the objectives of CFPA section 1033 for a third party to consider collection, use, or retention of data for these purposes to be within the scope of the consumer's requested product or service for purposes of proposed § 1033.421(a)(1).

The CFPB explained that proposed § 1033.421(a)(2) would not prevent third parties from engaging in the specified activities as standalone products. To the extent the core function that the consumer seeks out in the market is such an activity, a third party could potentially provide that core function to the consumer consistent with, and subject to, the terms of the proposed rule. Any such offering would be subject to other applicable laws, including the CFPA's prohibition on unfair, deceptive, and abusive practices.

Comments received

Commenter feedback on the proposed limitation on targeted advertising, cross-selling of other products or services, and data sales was varied. Some consumer advocates, data providers, and trade associations representing data providers expressed support for the proposed limitation in § 1033.431(a)(2). For example, some trade associations representing data providers stated that dark patterns or other deceptive practices from third parties result in consumers giving consent to activities consumers are not aware of, especially related to data sales and targeted marketing, and that requiring third parties to separately follow the authorization procedures to obtain consumer authorizations for these activities would be beneficial to consumers. An individual commenter similarly stated that consumers should not become subject to "surveillance capitalism" through authorization of third parties' use of covered data.

Various commenters, including trade associations for data providers, data providers, trade associations for nondepositories, data aggregators, consumer advocates, and others, appeared to

have different understandings about whether the proposed limitation in § 1033.421(a)(2) would prohibit consumers from authorizing their data to be accessed for these purposes. Some commenters appeared to interpret the proposal as a prohibition on such authorization. Others appeared to understand the proposal as permitting third parties, using covered data pursuant to consumer authorization, to engage in targeted advertising, cross-selling, and data sales as standalone products the consumer seeks out in the market. At least one trade association for data providers appeared unsure if the proposal would prohibit these activities, stating that the meaning of the phrase in the rule "any other product or service" is unclear.

Various commenters, including data providers, trade associations for data providers, consumer advocates, and other trade associations, asked for definitions of targeted advertising, cross-selling, and data sales. A consumer advocate and a trade association representing data providers proffered potential definitions. These commenters suggested that, without clarity on the bounds of these terms, the rule would lack sufficient clarity because the terms have broad and varied meaning in the market. For example, these commenters said the term targeted advertising is potentially broad and could cover advertising that uses consumers' personal characteristics and could also potentially include other concepts like contextual marketing that does not require precise identifiers. These commenters were also concerned about the definition of cross-selling because, as described by these commenters, the term could include some traditional attributes of personal financial management services that offer recommendations to consumers. A data provider commenter noted that the CFPB has not previously defined cross-selling of other products or services or data sales. A consumer advocate commenter suggested that the CFPB define data sales as the "sale, rental, exchange, or other transfer or use not otherwise authorized." Finally, two trade associations representing data providers requested that the CFPB develop a

clear concept or definition of what "any other product or service," means, and what "standalone product" means, as these terms may not have been clear in the proposed rule.

Some commenters, including research organizations and third parties, expressed concern that proposed § 1033.421(a)(2) might result in a prohibition on targeted ads, cross-selling, and data sales because, at least in some circumstances, they may not be traditionally offered as standalone products or services. A research organization and a third party commenter stated that the proposal might preclude third parties from using covered data for these purposes where they are traditionally a component of a product or service and are not standalone products or services. These commenters offered examples of products or services that might benefit consumers and might include targeted advertising or cross-selling. Some commenters, like trade associations for nondepositories, third parties, research institutes, consumer advocates, and data aggregators, asserted that proposed § 1033.421(a)(2) could result in consumer harms, such as higher prices, hindered choice, and others. These commenters expressed concerns about competition harms, like increased barriers to market entry for new companies who would traditionally rely on targeted advertising and cross-selling to generate growth, decreased innovation of new products, services, or business models, and increased consolidation in existing market players. These commenters stated that the CFPB did not account for the benefits to consumers through targeted advertising and cross-selling, and overstated potential harms. For example, some of these commenters cited studies they characterize as showing that consumers consistently authorize targeted advertising when given choices, significantly benefit from targeted advertising, and benefit from the competition that targeted advertising generates within the market.[101]

[101] *See, e.g.*, J. Howard Beales & Andrew Stivers, *An Information Economy Without Data*, at 15-16 (Nov. 2022); Patrick Grieve, *Personalized Customer Service: What It Is and How to Provide It*, ZenDesk (Feb. 2023), https://www.zendesk.com/blog/start-providing-personalized-customer-service/; Holly Pauzer, *71% of Consumers*

Some trade associations and third parties stated that the proposed limitation on targeted advertising, cross-selling of other products and services, and data sales would not ensure consumers are able to consent to third party products or services consumers might want and would therefore be a restriction on consumer choice. A trade association for nondepositories also stated that, if a consumer consents to third party collection of covered data for certain uses, like targeted advertising, then a prohibition on that use would run afoul of the First Amendment.

Finally, some commenters, including trade associations for nondepositories, a law firm, third party commenters, and data aggregators suggested that proposed § 1033.421(a)(2) is contrary to the congressional intent of CFPA section 1033 to ensure consumers can access data to use for their own preferences. These commenters stated that the CFPB generally lacks authority to prescribe limitations on the use of covered data, especially as it relates to targeted advertising, cross-selling of other products and services, and data sales. These commenters also objected to the CFPB's rationale for these proposed provisions and stated that the proposed rule did not evidence reasoned decision making or meaningful consideration of the consequences of intrusion into private, consent-based consumer relationships with third parties. Specifically, a trade association and law firm stated that CFPA section 1033 provides consumers an affirmative right to access their financial data but does not permit the CFPB to limit a third party's collection, use, and retention of covered data if the consumer has agreed to it. These commenters also stated that Congress intended that representatives acting on behalf of consumers would adhere to principles of agency law, which they said would result in authorizations from

---

Prefer Personalized Ads, Adlucent (2016), https://www.adlucent.com/resources/blog/71-of-consumers-prefer-personalized-ads/; Yan Lau, *A Brief Primer on the Economics of Targeted Advertising*, FTC 11–12 (Jan. 2020), https://www.ftc.gov/system/files/documents/reports/brief-primer-economics-targeted-advertising/economic_issues_paper_-_economics_of_targeted_advertising.pdf; Bus. Wire, *ICSC's Small Business Consumer Survey Reveals the Ongoing Importance of Small Businesses in the Lives of Consumers and Communities in the U.S.* (May 2, 2022), https://bwnews.pr/3rZ2KF3.

consumers to third parties that would carry regardless of whether the consumer benefits from the authorization. These commenters stated that if the consumer agrees to terms of data access, then the third party is acting on the consumer's behalf.

Final rule

For the reasons discussed herein, the CFPB is finalizing § 1033.421(a)(2) with minor modifications. Final § 1033.421(a)(2) provides that, for the purposes of the general limitation standard § 1033.421(a)(1), the following are not part of, or reasonably necessary to provide, any other product or service: (i) targeted advertising; (ii) cross-selling of other products or services; or (iii) the sale of covered data. For clarity, the CFPB is removing the term "activities" from the text of final § 1033.421(a)(2) and replacing the term with "purposes" in that provision's heading.

With respect to commenter concerns regarding consumer authorization for the purposes listed in § 1033.421(a)(2), the CFPB notes that § 1033.421(a)(2) does not prevent third parties from obtaining authorizations from a consumer to collect, use, and retain their covered data for any one of these specified purposes if offered as a standalone product or service. To the extent that the consumer seeks a product or service in the market which functions as targeted advertising, cross-selling of other products or services, or the sale of covered data, a third party could obtain a consumer's authorization to collect, use, and retain their covered data to provide that product or service to the consumer consistent with, and subject to, the terms of subpart D of part 1033.[102] Collection, use, and retention of covered data to provide such a product or service would be subject to other applicable laws, including the CFPA's prohibition on unfair, deceptive, and abusive practices.

[102] The CFPB has previously issued guidance related to commingling of targeting and delivery of advertisements to consumers. *See generally* Consumer Fin. Prot. Bureau, *Limited Applicability of Consumer Financial Protection Act's 'Time or Space' Exception With Respect to Digital Marketing Providers*, 87 FR 50556 (Aug. 17, 2022).

To be a "standalone" product or service, it must be clear that the targeted advertising, cross-selling, or sale of covered data is a distinct product or service the consumer could obtain in the market without obtaining other products or services.[103] As such, one provider could offer multiple products to a consumer, including targeted advertising, cross-selling, or sale of covered data as standalone products, obtain separate authorizations for consumer's data to be used for those products or services, and provide those products or services to the consumer. This would be similar to a bank that may offer checking accounts, savings accounts, and credit cards to a consumer, even while allowing those services to be managed on one banking app.

Further, as described in the proposed rule, the CFPB is concerned that consumers do not seek in the market targeted advertising, cross-selling of other products and services, and data sales.[104] Commenters suggested that consumers can significantly benefit specifically from, and continue to sign up for, targeted advertising and cross-selling in various contexts. As described

[103] As described above related to the consumer's requested product or service, the CFPB does not intend to suggest a "standalone product or service" would necessarily have only a single attribute. While many standalone products or services might have only one attribute, as in cases where third parties sell covered data, others may have more than one attribute. A third party might provide to consumers a standalone product or service of targeted advertising, which could have multiple attributes to ensure the consumer is receiving the product or service they would expect. For example, a "standalone product" that involves targeted advertising might both evaluate a consumer's data for the purpose of identifying lower cost credit cards for a particular consumer and send that consumer advertisements for such lower cost credit cards.

[104] *See, e.g.*, Rodney John Garratt & Michael Junho Lee, *Monetizing Privacy*, at 4, Fed. Rsrv. Bank of N.Y. Staff Rep. No. 958 (Jan. 2021), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr958.pdf (stating that "[m]ost of the gains from consumer data do not go to consumers"); Raheel A. Chaudhry & Paul D. Berger, *Ethics in Data Collection and Advertising,* 2 GPH Int'l J. Bus. Mgmt. 1, 5-6 (2019), http://www.gphjournal.org/index.php/bm/article/view/240/110 (stating that targeted advertising and data monetization allow companies to collect, use, and retain "consumer data without the user being any the wiser," and that targeted advertising and data monetization elevate "the risk involved in data breaches and malicious parties buying consumer data on the secondary data market"); Yan Lau, *A Brief Primer on the Economics of Targeted Advertising,* Bureau of Econ., Fed. Trade Comm'n, at 9-10 (2020), https://www.ftc.gov/system/files/documents/reports/brief-primer-economics-targeted-advertising/economic_issues_paper_-_economics_of_targeted_advertising.pdf (describing that, while consumers can benefit from targeted advertising, there are multiple consumer harms that result from targeted advertising, such as: consumers may underestimate the "degree and consequence of the personal data collection websites carry out in exchange for providing free digital goods and services"; consumers may feel the benefits of targeted advertising do not outweigh the "perceived intrusiveness of the advertising"; and consumers may experience harms related to data breaches or misuse of their data).

above, commenters provided some evidence that consumers sign up for targeted advertising and cross-selling and receive certain benefits from them. Other research suggests that any such benefits are uncertain at best and may be difficult to quantify. Regardless, the CFPB recognizes that consumers might continue to sign up for, and in some cases can benefit from, targeted advertising, cross-selling, and data sales. However, this does not indicate that consumers understand the consequences of third parties using data for these purposes,[105] are the primary beneficiary of collection, use, and retention for these purposes,[106] or that consumers specifically sought them out.[107] Instead, this might indicate that consumers have little choice but to sign up for, or unknowingly or reluctantly acquiesce to, targeted advertising and cross-selling to receive more preferable or free services.[108]

---

[105] *See generally* Brooke Auxier *et al.*, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Rsch. Ctr. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (describing findings that only "one-in-five adults overall say they always (9 percent) or often (13 percent) read a company's privacy policy before agreeing to it" and that 59 percent say "they understand very little or nothing about" what companies do with data they collect); Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 Wash. U. L. Rev. 1461, 1479 (2019), https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6460&context=law_lawreview ("[F]ar too often, far too many people in the digital environment have little to no idea about what data practices or exposure that they are consenting to.").

[106] *See generally* Eduardo Abraham *et al.*, *Behavioral Advertising and Consumer Welfare: An Empirical Investigation*, SSRN Elec. J., at 2 (2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4398428 ("[L]ittle is known about the manner and extent to which targeted ads affect consumers' welfare. In fact, the relationship between a product being associated with targeted ads and its price, quality, or novelty . . . has not been explored. Some models suggest that, if consumers had to make a voluntary decision to provide personal information to advertisers, only those who benefit from it would do so, and therefore targeted advertising should be strictly beneficial to them.").

[107] *See generally* Charlotte A. Tschider, *Meaningful Choice: A History of Consent and Alternatives to the Consent Myth*, 22 N.C. J. L. & Tech. 617, 635-37, 639 (2021) (explaining that while consumers might consent to certain activities presented to them, their consent might not reflect autonomous choice from the consumer or the consumer's desires).

[108] *See* April Falcon Doss, *Cyber Privacy*, at 54 (BenBella Books, Inc. 2020) (explaining that the business model of companies that monetize consumer data are able to exploit information asymmetries and bargaining power imbalances such that, even if a consumer has a higher risk tolerance and is willing to share more data for the purposes of monetization of that data, digital platforms offer consumers very little choice to exercise those preferences); Charlotte A. Tschider, *Meaningful Choice: A History of Consent and Alternatives to the Consent Myth*, 22 N.C. J. L. & Tech. 617, 637 (2021) (positing that consumers who consent to products or services might struggle to understand the differences of primary uses from secondary uses where the two are bundled into contracts of adhesion, of which consumers might only want some aspects but not all of what they authorized).

The CFPB understands that it is possible for consumers to benefit from targeted advertising, cross-selling, and data sales and the final rule ensures that consumers can authorize their covered data to be collected, used, and retained for these purposes, with provisions to ensure consumers are able to make a meaningful choice to do so.[109] The final rule recognizes that consumers should not have to unknowingly or reluctantly acquiesce to their covered data being collected, used, and retained for these purposes in order to receive a product or service they have sought in the market. As such, the CFPB affirms that, under the final rule, consumers can authorize their data to be collected, used, and retained for targeted advertising, cross-selling, or data sales if offered as standalone products or services—this authorization simply cannot be combined in one authorization for data access for other products or services.

As noted above, some commenters stated that proposed § 1033.421(a)(2) was contrary to the congressional intent of CFPA section 1033 to ensure consumers can access their own data for their own preferences. These commenters also stated that the proposed rule would otherwise result in a restriction of consumer choice. However, § 1033.421(a)(2) does not restrict consumer choice or inhibit consumers from accessing their data for their own preferences. Under the final rule, third parties can, pursuant to consumer authorization, collect, use, and retain covered data to provide, targeted advertising, cross-selling of other products or services, or data sales as standalone products or services.

[109] *See generally* Alessandro Acquisti *et al.*, *Behavioral Advertising and Consumer Welfare*, at 16 (2023), https://dx.doi.org/10.2139/ssrn.4398428 ("The results suggest that a search will, on average, make consumers who are price focused and have low search costs (relative to the price of the product) better off. These results also highlight that display advertisements may be a useful channel for smaller vendors to reach consumers: some of these vendors may seldom (if ever) appear in organic search. Such results highlight the complex nature of consumer welfare effects from targeted advertising. If search costs are sufficiently low and consumers are generally aware of the product categories which interest them, targeted ads are unlikely to improve their surplus. Surplus gains are even less likely to accrue to consumers if they need to vet the lesser known vendors that appear in display advertising. More than likely, this additional effort is better used seeking out relevant products via traditional search.").

As described above, a trade association for nondepositories argued that the provision related to cross-selling, targeted advertising, and data sales would violate the First Amendment's protections on commercial speech if it prohibited data to be collected, used, and retained by third parties for these purposes when a consumer otherwise consents. However, the final rule does not infringe on any First Amendment rights. Even assuming the final rule could be construed to restrain speech, it would readily survive the applicable standard of scrutiny for commercial speech. Under the Supreme Court's commercial speech framework, if the speech is not misleading and relates to lawful activity, the government may impose restrictions that advance a substantial government interest and are no more extensive than is necessary to serve that interest. As explained elsewhere, the final rule advances several substantial interests, including the need for consumer control of personal financial data and privacy protections. The requirements set forth in the rule are also appropriately tailored to achieve these interests. As previously noted, the CFPB affirms that collection of covered data for certain uses, including cross-selling, targeted ads, and data sales, may be separately authorized as a standalone product or service. This regulatory structure provides the appropriate balance to ensure consumers are given a meaningful choice before engaging in targeted advertising, cross-selling, and data sales, and that they are shielded from signing up for purposes that they do not understand or do not request.

Additionally, as described above, commenters asked for and suggested definitions for targeted advertising, cross-selling of other products or services, and data sales. For the purposes of § 1033.421(a)(2), the CFPB intends to take the position that targeted advertising is advertising that comprises the identification or selection of prospective customers or the selection or placement of content to affect consumer engagement, including purchase or adoption behavior. Cross-selling of other products and services is the advertising, sale, or referral of the third party's

own products or services to the third party's existing customers. Data sales is selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating personal information for monetary or other valuable consideration.

Limitations on collection of covered data (§ 1033.421(b))

Proposed § 1033.421(b) contained third party obligations related to collection of covered data. Under proposed § 1033.421(b), as a condition of being authorized to access covered data on a consumer's behalf, the third party would be required to (1) limit its collection of covered data, including the scope of covered data, to what is reasonably necessary to provide the consumer's requested product or service, consistent with § 1033.421(a); (2) limit the duration of collection of covered data to the maximum durational period; (3) obtain a new authorization from the consumer, in a reasonable manner, to collect covered data beyond the maximum durational period; and (4) abide by certain limitations on collection, use, and retention of covered data beyond the maximum durational period if the third party does not obtain a new authorization from the consumer.

The specific provisions of § 1033.421(b) are discussed below.

In general (§ 1033.421(b)(1))

Proposed § 1033.421(b)(1) stated that, for purposes of the general limitation on collection, use, and retention of covered data in proposed § 1033.421(a), collection of covered data would include the scope of covered data collected and the duration and frequency of collection of covered data.

Some commenters, including consumer advocates, data providers, trade associations for data providers, and research organizations, stated general support for the proposed limitations on collection. Some commenters, including consumer advocates and third parties, suggested that

consumers should have more control than what the proposed rule would have required over how long and how often third parties collect covered data, and that the proposed standard to limit collection might not adequately account for third parties' ongoing relationships with consumers. Other commenters, particularly data providers and third parties, suggested that data providers should have a role in ending third party access if collection exceeds the scope of the consumer's authorization.

For the reasons discussed herein, the CFPB is generally finalizing § 1033.421(b) as proposed, with one modification. The CFPB has determined that third parties are the commercial actors in the best position to understand the covered data they need to collect from the data provider to facilitate provision of products or services, and to therefore limit that collection to only what is reasonably necessary to provide the consumer's requested product or service. The CFPB has also determined that the standard to limit collection to what is reasonably necessary provides third parties with sufficient flexibility to account for the needs of the requested product or service.

The CFPB is revising the language of proposed § 1033.421(b)(1) to state that collection includes the scope of covered data "requested," instead of the proposed "collected." This clarifies that, in certifying to limit the collection of covered data pursuant to § 1033.421(a), third parties must tailor their request for covered data to only what is reasonably necessary to provide the consumer's requested product or service.

The CFPB notes that, in some circumstances, the third party might receive from the data provider more data than the third party requests. For example, this could happen when, pursuant to § 1033.211(d), the third party requests terms and conditions data from the data provider and the data provider provides more data elements than the third party requested, or more than is

reasonably necessary to provide the consumer's requested product or service consistent with § 1033.421(a). Additionally, third parties could receive data after a consumer has revoked the third party's access to the data pursuant to § 1033.421(h), before the data provider has processed the request. In circumstances where the third party receives more data than they request, the general limitation on use and retention in § 1033.421(a) would not allow third parties to use that data if such use is not reasonably necessary. Section 1033.421(a) would allow a third party to retain covered data for as long as reasonably necessary to locate and delete the data.

Further, pursuant to the certifications related to collection in § 1033.421(a) and (b), if a third party receives information that indicates the consumer may no longer expect to receive the product or service, the third party should confirm collection of covered data remains reasonably necessary.

Maximum duration (§ 1033.421(b)(2))

Under proposed § 1033.421(b)(2), third parties would be required to certify to limit the duration of collection of covered data to a maximum period of one year after the consumer's most recent authorization. The proposed rule described this as the maximum durational limit.

Regarding the maximum durational limit, the proposed rule noted that some products or services, like bill pay, overdraft prevention, or personal financial management, require long-term access. For such products or services, the proposed rule stated that the general limitation standard may not be sufficient to ensure that third parties act on behalf of consumers when collecting data longer term. The proposed rule stated that consumer needs or expectations may change in ways that may not be apparent to the third party, as could happen when a consumer stops using a product or service and forgets that they authorized third party data access. The proposed rule stated that, in other cases, consumers may have attempted to end third party access without

actually doing so, such as when a consumer deletes an application from a device with the intent of stopping data collection, use and retention. At the same time, the proposed rule also acknowledged that there are other cases where consumers request products or services that require long-term data collection and want to authorize ongoing third party data access. In those cases, the CFPB preliminarily determined that it would frustrate consumer intent and burden third parties to terminate third party access or require frequent reauthorizations. The proposed rule stated that a maximum durational limitation would provide a helpful backstop on the duration of third party authorization for these consumers.

Comments were mixed between supporting the proposed provision and recommending changes. Commenters that supported a maximum durational limitation, mostly banks, credit unions, community banks, trade associations for data providers, and research institutes, stated that such a limit promotes consumer control by requiring third parties to seek periodic reauthorization. Commenters that were critical of the proposal to impose a maximum durational period, mostly third parties, trade associations for third parties, and consumer advocates, stated that, if implemented, a maximum duration requirement would ultimately result in consumer harms, like: increased and unhelpful friction because of required reauthorization; disruption of valuable products and services that require ongoing collection, use, and retention in cases where consumers do not reauthorize; and disruption to the user experience if consumers utilize a product or service continually but must still reauthorize.

Commenters who supported a one-year maximum duration limitation commended the provision for reducing friction as compared to other privacy regimes that require shorter durational periods and therefore increased requests for reauthorization. In contrast, a trade association for third parties stated the CFPB did not provide adequate support for the proposed

one-year maximum durational period and would not be consistent with the consumer's consent for the third party to continually collect their data. A data aggregator suggested amending the maximum durational period to 13 months, rather than 12, to better account for products and services that may have a slightly longer cycle of relevance for consumers, like tax preparation software. Further, various third parties and trade associations for nondepository commenters suggested the CFPB account for payments products or services through more narrow or more flexible durational limits, including by incorporating flexibilities based on the consumer's use of the product or service. These commenters suggested consumer authorization should last as long as consumers actively use the product or service, or suggested other activity-based flexibilities or restrictions. Finally, a trade association for community banks stated that the final rule should make clear that the general limitation standard of reasonable necessity would mean many short-term products and services would end before the maximum durational period ends.

For the reasons discussed herein, the CFPB is finalizing in § 1033.421(b)(2) a maximum durational limit of one year after the consumer's most recent authorization. This approach protects consumers by helping prevent unwanted, long term data collection, and also ensures consumers are able to periodically revisit the authorizations they have provided to third parties and ensure third party data access reflects consumers' wishes. Specifically, the one-year durational limit provides a helpful backstop to consumers who sign up for products or services that include ongoing data collection. For these reasons, the CFPB declines to allow for authorizations longer than 12 months when a consumer is actively using a product or service, as requested by some commenters. While, as described above, some commenters raised concerns about added friction for consumers related to a maximum durational limit, some of this friction is a necessary and helpful aspect of the consumer's relationship with the authorized third parties, as

it provides consumers opportunities to carefully consider their choices. The maximum durational limit and the general obligation to limit collection to what is reasonably necessary to provide the consumers' requested product or service account for the wide variety of products or services the consumer might seek. For products or services that necessitate shorter durations of collection, like traditional underwriting and identity verification, the general data limitation standard will result in collection of covered data for a shorter period than one year. And, as noted above and in the proposed rule, consumers benefit from a one-year maximum durational period in cases where the general limitation standard may not be sufficient to ensure that third parties act on behalf of consumers when collecting data longer term.

Reauthorization after maximum duration (§ 1033.421(b)(3))

Under proposed § 1033.421(b)(3), the third party would certify that, to collect covered data beyond the one-year maximum durational period, the third party would obtain a new authorization from the consumer no later than the anniversary of the most recent authorization from the consumer. Under the proposed rule, the third party would be permitted to ask the consumer for a new authorization in a reasonable manner. The proposed rule stated that indicia that a new authorization request would be reasonable would include its conformance to a qualified industry standard.

The proposed rule stated that consumers would benefit from the combination of a maximum durational limit of one year and from the control that reauthorization requirements might provide. The proposed rule further stated that the CFPB preliminarily determined that third parties might need to seek new authorizations multiple times or otherwise explain to consumers why they are seeking new authorizations, but that this might unnecessarily burden consumers if they receive too many requests, or requests for products or services they no longer want. The

proposed rule stated that the CFPB sought to strike a balance between these competing considerations. The proposed rule also acknowledged that additional guidelines regarding reauthorization requests might facilitate compliance. As such, the proposed rule stated that indicia that a new authorization request is reasonable include its conformance with a qualified industry standard.

Some commenters—including banks, trade associations for credit unions, and third parties—offered support for the proposed reauthorization provision, stating that consumers often forget about their connections and could benefit from opportunities to reauthorize. Some data aggregators, trade associations for banks, consumer advocates, and research organizations did not clearly oppose the proposed rule but offered narrow critiques or suggested changes, discussed below.

Some trade associations for third parties and data aggregators expressed concern that consumers would not provide a new authorization at the end of a maximum duration limit when they might otherwise want their authorizations to continue, which could result in harm to consumers. For example, one third party suggested that if a consumer never reauthorizes, the consumer might be directly harmed by the cut-off of the maximum durational period before the consumer accrues the benefits of long-term data collection.

Commenters' suggested modifications, clarifications, or additions to the implementation of reauthorization include: specify in the rule that a consumer's most recent authorization includes when a consumer requests a third party to refresh their data, or every time a payment goes through; finalize more specific limitations for requesting reauthorization, including limiting pop-ups and notices, the number of requests, or requests that could be threatening, misleading, or otherwise negatively impact consumers; allow the consumer to provide more streamlined

reauthorizations as compared the initial authorization, or fewer reauthorization for certain products or services with which consumers regularly interact, like peer-to-peer or periodic payment products; allow flexibility for reasonable reauthorization methods, including directly to consumers via electronic means; allow third parties to simply notify the consumer of ongoing collection, use, and retention; and clarify the reasonable manner requirement related to reauthorization.

For the reasons discussed herein, the CFPB is finalizing § 1033.421(b)(3) as proposed with a terminology change to conform to the final rule's use of the term "consensus standard." Specifically, final § 1033.421(b)(3) provides that, to collect covered data beyond the one-year maximum period described in § 1033.421(b)(2), the third party will obtain a new authorization from the consumer pursuant to § 1033.401 no later than the anniversary of the most recent authorization from the consumer. Final § 1033.421(b)(3) further provides that the third party is permitted to ask the consumer for a new authorization pursuant to § 1033.401 in a reasonable manner. Final § 1033.421(b)(3) further provides that indicia that a new authorization request is reasonable include its conformance to a consensus standard.

The CFPB acknowledges that this approach may result in some increased friction for consumers, but it will also allow consumers to periodically confirm their previous choices, including that they continue to want the third party to access their data for the requested product or service. Commenters appeared to assume that consumers generally will not reauthorize at the end of one year, but did not provide evidence that consumers, on the whole, will not reauthorize after a maximum duration period of one year, at least in circumstances in which they want data access to continue. As such, after considering this feedback, the CFPB is not making changes to the proposed reauthorization requirement.

Some commenters suggested the final rule should allow third parties to provide streamlined reauthorization requests to consumers, including suggesting that facilitated payments could serve as periodic reauthorizations for consumers. The CFPB has determined that consumers could benefit significantly from the authorization procedures as described in § 1033.401, including the authorization disclosure, and that streamlined reauthorization procedures would not effectively ensure consumers remain informed and in appropriate control of data access. The CFPB is thus not adopting commenters' suggested modifications to streamline reauthorization requests.

Effects of maximum duration (§ 1033.421(b)(4))

Proposed § 1033.421(b)(4) would have required the third party to certify that, if a consumer does not provide a new authorization before the maximum durational periods, the third party would (1) no longer collect covered data pursuant to the most recent authorization, and (2) no longer 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 under proposed § 1033.421(a). The CFPB is finalizing these provisions, without substantive change, in § 1033.421(i), discussed below. Comments regarding proposed § 1033.421(b)(4) are discussed in detail below related to § 1033.421(i).

Limitations on use of covered data (§ 1033.421(c))

Proposed rule

As discussed above, the CFPB proposed in § 1033.421(a) that, to be authorized to access covered data, a third party must certify to using covered data only as reasonably necessary to provide the consumer's requested product or service. Preamble to the proposed rule explained

that use of covered data that is not reasonably necessary to provide the consumer's requested product or service would be "secondary use," and would not be permitted as part of the third party's authorization to access the consumer's covered data. The proposed rule specified in § 1033.421(c) that, in addition to limiting the third party's own use of covered data, third parties would not be able to provide covered data to other third parties unless doing so would be reasonably necessary to provide the consumer's requested product or service.

Further, for clarity, proposed § 1033.421(c) provided the following examples of uses of covered data that would be permitted as reasonably necessary under proposed § 1033.421(a): (1) uses that are specifically required under other provisions of law, including to comply with a properly authorized subpoena or summons or to respond to a judicial process or government regulatory authority; (2) uses that are reasonably necessary to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; and (3) servicing or processing the product or service the consumer requested. The proposed rule stated that these examples would provide third parties with additional clarity on how the limitation standard would apply with respect to certain business activities. The CFPB sought feedback on whether it should include in the final rule other examples of business activities that are reasonably necessary to provide consumer requested products or services.

The proposed rule also sought feedback on whether the final rule should permit third parties to solicit consumers' opt-in consent to some secondary uses of consumer data to provide flexibility to third parties while maintaining important consumer protections. For example, the proposed rule sought feedback on whether the final rule should permit third parties to solicit consumers' opt-in consent to secondary uses as part of a third party's authorization to access covered data, while requiring third parties to certify not to use covered data for certain higher-

risk secondary uses. The proposed rule also sought feedback on whether the final rule should permit third parties to solicit a consumer's opt-in consent to engage in secondary uses with de-identified data, and if so, what de-identification standard the rule should provide. The proposed rule sought feedback on how any opt-in approach could be structured to ensure that consumers are providing express informed consent to any secondary data uses, and whether the proposed authorization disclosure would be an appropriate vehicle for soliciting granular consumer choices about data use, such as through a secondary use opt-in mechanism. Finally, the proposed rule sought feedback on how opt-in mechanisms could be implemented to prevent third parties from using "dark patterns" or deceptive practices aimed at soliciting consumer consent.

Comments received

Commenter feedback on the proposed limitation on use was varied. Regarding the examples in proposed § 1033.421(c), many commenters, including third parties and third party trade associations, privacy organizations, Members of Congress, and data aggregators, requested that the CFPB specify additional uses that would be permissible under the final rule. Other examples of additional uses that commenters requested the CFPB specify in the final rule included product improvement, new product development, prevention of crime or illegality, offering beneficial products or services to consumers, supplemental primary uses, reporting of data, and internal and external research. Some research institutes, a third party, and a trade association raised concerns about the proposed examples of reasonably necessary uses set forth in proposed § 1033.421(c), and specifically raised concerns that the example for servicing or processing the consumer's requested product or service was too narrow. These commenters suggested additions that would broaden that example, like "assessing the consumer's eligibility for or delivering, servicing, or processing the product or service the consumer requested,"

allowing third parties to service or process products or services on which the consumer's requested product or service relies, or providing more elaboration or clarification about the meaning of servicing or processing.

Regarding the proposed limitation on secondary uses, a wide range of commenters, including data providers, consumer groups, and research organizations, were generally supportive of strong restrictions on secondary use, but most commenters asserted that the proposed secondary use limitation would be overly restrictive. Many commenters stated that a prohibition on secondary use, without modification and limited exceptions, would negatively affect product innovation, overly restrict consumer choices for potentially beneficial products, and put third parties at a significant competitive disadvantage to data providers that are unrestricted by the limitation. Some of these commenters suggested alternative approaches, including categories of permissible uses that are not primary or secondary. Some third parties, Members of Congress, and research institutes raised concerns about how a strict limitation on secondary uses might impact beneficial products or services for consumers, like cash-flow underwriting. Some third party commenters requested that the final rule permit more expansive uses related to fraud prevention. And many third parties asserted that the proposed secondary use restrictions would harm consumers and raise costs or reduce revenues for third parties. They stated that such restrictions would reduce competition and innovation, limit their ability to detect and prevent fraud, and prevent third parties from improving their products and services. Some commenters asserted that the prohibition on secondary use would be an outlier among existing privacy regimes. A few third party commenters recommended that the final rule allow uses that are also permitted by the GLBA and Regulation P because, these commenters claimed, different use limitations would unfairly disadvantage third parties and confuse consumers.

Commenters suggested a range of revisions to address these concerns in the final rule, including that the CFPB permit some secondary uses, like those listed above, and should more strictly prohibit some specific uses. For example, some commenters, like data providers and trade associations for data providers, stated that the CFPB should specifically prohibit certain uses, like uses of data for reverse engineering of proprietary algorithms.

Some commenters, including third parties, third party trade associations, and some privacy organizations, advocated for the final rule to permit consumers to opt into secondary data uses. These commenters stated that opt-in consents would benefit consumers and could increase consumer control over the uses of their data. Some of these commenters identified certain high-risk uses to which consumers should not be permitted to opt in. For example, consumer advocates and trade associations stated that certain types of loans that have resulted in enforcement actions, targeted marketing for predatory products, uses of wealth indicators that result in discriminatory algorithms, and behavioral insights derived from location, among others, are high risk uses that should not be permitted under the final rule, even through opt-in consent. And one trade association for data providers also stated that financial institutions, when acting as third parties, should be permitted to solicit opt-ins from consumers for some secondary uses of covered data, because such institutions must adhere to regulations to maintain sensitive data.

Other commenters, including third parties, data aggregators, trade associations, and research institutes, offered support for an opt-out option for consumers, citing examples from other privacy regimes that rely on opt-out mechanisms. These commenters stated that third parties should permit consumers to opt out of secondary uses that would be allowed in certain contexts, like when compatible with the product or service or through streamlined consent frameworks that benefit consumers. A data aggregator provided an example of a third party

cross-selling a savings account to a consumer who already has a checking account with the third party, and stated that consumers should be able to opt out from these kinds of secondary uses.

In contrast, some commenters, including research institutes and third parties, expressed caution about an opt-in or opt-out approach. For example, a research institute stated that consumers presented with granular choice options would experience choice overload and decision paralysis and elect not to proceed with a transaction.[110] A third party stated that authorizations for any secondary uses should include enhanced disclosure requirements and should prohibit other parties from additional secondary uses, and suggested that these kinds of protections are not compatible with opt-in methods. A research institute stated that evidence shows opt-in consents result in significantly reduced participation rates.[111] Some commenters recommended that the final rule address concerns about the secondary use proposal being overly restrictive through additional clarifications of reasonably necessary uses and exceptions for certain secondary uses. Further, commenters stated that there might be significant limits to the benefits of opt-in approaches. For example, as described in more detail below, a group of academic researchers and consumer advocates stated their concerns that employing opt-ins for research might significantly degrade the quality of the data.

---

[110] *See generally* Alexander Chernev *et al.*, *Choice Overload: A Conceptual Review and Meta Analysis* (2015); Choice Overload, https://www.researchgate.net/publication/265170803_Choice_Overload_A_Conceptual_Review_and_Meta-Analysis.

[111] *See generally* Joseph W. Sakshaug *et al.*, *Evaluating Active (Opt-In) and Passive (Opt-Out) Consent Bias in the Transfer of Federal Contact Data to a Third-Party Survey Agency*, 4 (3) J. Survey Stats. & Methodology, at 382-416 (Sept. 2016), https://www.researchgate.net/publication/307625870_Evaluating_Active_Opt-In_and_Passive_Opt-Out_Consent_Bias_in_the_Transfer_of_Federal_Contact_Data_to_a_Third-Party_Survey_Agency; and Yvonne de Man, Ph.D. *et al.*, *Opt-In and Opt-Out Consent Procedures for the Reuse of Routinely Recorded Health Data in Scientific Research and Their Consequences for Consent Rate and Consent Bias: Systematic Review*, J. Med. Internet Rsch. (Feb. 2023), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10015347/.

Many commenters addressed the use of de-identified data by third parties. Numerous commenters, including research organizations, consumer advocates, and third parties, supported allowing third parties to use de-identified data for secondary purposes. These commenters stated that de-identified data enables a variety of uses that benefit consumers. For example, commenters said that de-identified data allows businesses to develop new products and services, improve existing products and services, and improve account security and fraud prevention. Commenters also said that de-identified data allows for research that serves the public interest. For example, a third party and a data aggregator commenter said that third parties had shared de-identified data with government agencies to improve policymaking. A research institute commenter stated that the CFPB's Consumer Credit Panel and credit card agreement database use de-identified data. However, a consumer advocate commenter stated that even de-identified data could be exploited for commercial ends like marketing, and therefore recommended limiting the use of de-identified data to research purposes.

Some commenters addressed the consent standard that should apply to uses of de-identified data. Academic, research institute, and consumer advocate commenters stated that opt-in consent would impair the value of any de-identified data used for research purposes. These commenters stated that frequent opt-in requests could overwhelm consumers and that consumers who opt in to sharing their data are non-representative of the general population, which undermines the validity of any research based on such consumers. However, a government commenter and a consumer advocate commenter said that opt-out frameworks have been shown to minimize sample biases and preserve the utility of data in other research contexts. A data provider commenter said that opt-in consent should be required for any use of de-identified data.

Some third party commenters were concerned about what they described as anticompetitive effects of the proposed limitation on using de-identified data. For example, a research institute and several third party commenters said that new market entrants need access to de-identified data to train machine learning models or otherwise ensure that their products function properly. Third party commenters also said that the proposed rule would limit their use of covered data in ways that existing law does not limit data providers' use of the same data. One third party commenter stated that it was not fair that a bank could use de-identified data for nearly any purpose if obtained directly from a customer, but a third party could not use the same data for any secondary purposes if obtained under the rule as proposed.

Commenters also stated that allowing third parties to use de-identified data would also create consistency between the final rule to implement CFPA section 1033 and various State, Federal, and international privacy regimes. One research institute commenter stated that GLBA and FCRA allow greater flexibility in using de-identified data. Several commenters believed that U.S. businesses would face a competitive disadvantage if the final rule were more restrictive than the E.U. General Data Protection Regulation (GDPR).

However, a few data providers and trade associations for data providers opposed allowing third parties to use de-identified data for secondary purposes. Two bank commenters asserted that de-identified data could be re-identified, which would invade consumer privacy. In contrast, a research institute commenter stated that most high-profile examples of re-identification involved data that was never properly de-identified initially. This commenter also said that risks of re-identification were low if the data was limited to internal use and not shared with other third parties.

Final rule

For the reasons discussed herein, the CFPB is finalizing § 1033.421(c) with an additional example of reasonably necessary uses. Final § 1033.421(c) states that use of covered data for purposes of § 1033.421(a) includes both the third party's own use of covered data and provision of covered data by that third party to other third parties. Final § 1033.421(c) further states that examples of uses of covered data that are permitted under § 1033.421(a) include: uses that are specifically required under other provisions of law, including to comply with a properly authorized subpoena or summons or to respond to a judicial process or government regulatory authority; uses that are reasonably necessary to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; servicing or processing the product or service the consumer requested; and uses that are reasonably necessary to improve the product or service the consumer requested. The CFPB has determined that, generally, consumers expect covered data might be used for these purposes and that third parties will benefit from additional clarity, provided by these examples, on uses that are reasonably necessary to provide the consumer's requested product or service under the standard in § 1033.421(a). The examples in § 1033.421(c) are illustrative and are not comprehensive of uses of covered data that will be reasonably necessary under the general limitation standard.

The CFPB is aware that third parties might need to use covered data to comply with legal requirements or to protect against fraud, unauthorized transactions, and similar purposes. The final rule is not intended to restrict uses of covered data that effect compliance with applicable laws, like anti-money laundering laws or other applicable rules or regulations, or to block criminal law enforcement activity. For example, in many cases, it would be reasonably necessary for third parties to use basic account verification information to confirm that the consumer is

authorizing information from an account that does in fact belong to that particular consumer. One third party commenter explained that third parties might use covered data to determine the likelihood of consumers' future payments failing by monitoring past instances of consumers freezing their accounts or inability to transfer funds, describing those uses of data as being for fraud prevention purposes. The CFPB cautions that the example in § 1033.421(c)(2) is limited to uses to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability if such uses are reasonably necessary. The examples in § 1033.421(c) do not expand the scope the general limitation standard in § 1033.421(a) and, to be permissible, the uses described in the examples in § 1033.421(c) must be reasonably necessary in a given context.

After considering comments, the CFPB is finalizing in § 1033.421(c) an additional example of permitted uses of covered data: uses that are reasonably necessary to allow for improvement of the consumer's requested product or service. The CFPB agrees with commenters that the reasonably necessary standard of § 1033.421(a) would generally permit third parties to use covered data to improve the requested product or service. Generally, consumers expect that products or services they have requested that rely on consumer-permissioned data will be improved over time and, as such, the CFPB is finalizing this additional example in § 1033.421(c)(4) to provide clarity, which will assist third parties providing products and services that consumers request.

The CFPB considered commenters' suggestions to add other examples of uses that are permissible under the general standard in § 1033.421(a) but declines to do at this time. The CFPB believes the examples in the final rule provide sufficient guidance to third parties on uses that are permissible as reasonably necessary to provide the consumer's requested product or

service. The examples provided in the final rule are non-exhaustive, and other uses are permissible as reasonably necessary to provide the consumer's requested product or service.

The CFPB considered comments suggesting additional prohibitions related to certain uses, like uses of data for reverse engineering of proprietary algorithms, price discovery in capital markets, or behavioral monitoring and algorithm development. As stated in the proposed rule, uses that are not reasonably necessary to provide the consumer's requested product or service are secondary uses, and are not permitted as part of the third party's authorization to access the consumer's covered data for purposes of providing that product or service. Many of commenters' suggested additions would generally be considered secondary uses in as much as they would not be reasonably necessary to provide the consumer's requested product or service.[112] And other uses of covered data for the purposes of targeted advertising, cross-selling of other products or services, and data sales are sufficiently limited by the requirement in § 1033.421(a)(2) that those purposes are not part of, or reasonably necessary for, any other product or service and therefore must be offered as a standalone product.

The CFPB considered additional flexibilities, like providing consumers an opt-in to certain secondary uses or permitting secondary uses through the use of de-identified data. The CFPB agrees with commenters who described opt-in, or opt-out, approaches as not sufficiently protective to consumers. The CFPB declines to allow third parties, including financial institutions acting as third parties under this rule, to solicit opt-in or opt-out consents from consumers to use covered data obtained pursuant to consumer authorization for secondary uses. The CFPB is concerned that consumers might not receive adequate information through granular

[112] With respect to the comment suggesting the CFPB prohibit uses of data for reverse engineering of proprietary algorithms, the CFPB expects that such uses would not be reasonably necessary for a consumer's requested product or service. The CFPB will closely monitor the market to determine whether third parties are using covered data for these purposes.

choice mechanisms that would result in meaningful consent.[113] The CFPB is also concerned that if offered too many opt-in choices in the course of a single authorization process, consumers might experience decision fatigue or choice paralysis, and therefore might agree to terms they have not considered or instead might not complete authorization.[114] The CFPB also agrees with commenters' concerns regarding opt-in or other granular choice options for consumers, particularly related to de-identified data, as these choices might result in selection bias issues that make the use of the data consumers opted into sharing unhelpful for research purposes. Additionally, the CFPB is concerned that when consumers experience decision fatigue or choice paralysis, an opt-in or opt-out approach might result in greater data sharing than they would choose if in a position to make a considered choice. Generally, the authorization procedures pursuant to § 1033.401 are designed to ensure both that consumers understand the scope of a requested product or service and that third parties do not impermissibly expand the scope of their collection, use, and retention beyond what is reasonably necessary to provide that product or service. In addition, the rule does not prevent third parties from offering consumers more than one product by means of additional, separate authorizations that comply with subpart D. The CFPB determines that separate authorizations pursuant to the procedures in § 1033.401 will afford consumers with more meaningful consent to data access than consumers would have

[113] *See* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 Wash. U. L. Rev. 1461, 1479-1486 (2019), https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6460&context=law_lawreview (describing numerous ways in which a consumer might consent to choice options without understanding what they are authorizing); Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. Rev. 1687, 1734 (2020) (stating that even when the consumer is functioning under ideal circumstances when giving consent, consumers' ability to give informed and meaningful consent is finite and cannot scale to all the privacy choices a consumer must make).

[114] *See* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 Wash. U. L. Rev. 1461, 1484, 1486 (2019), https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6460&context=law_lawreview (describing how a consumer might experience decision fatigue if presented with detail to provide sufficient information to make granular choices).

through traditional opt-in requests, which the CFPB understands to combine requests for data access for a product or service the consumer is seeking with requests for consumer consent for data access for additional purposes. Such combined requests might not allow consumers to make considered choices to the same degree as separate authorizations, and therefore the procedures in § 1033.401 will provide consumers more control over their data access authorizations.

At this time, the CFPB is not including a provision that would allow third parties to use de-identified data for purposes that are not reasonably necessary to provide the consumer's requested product or service. As discussed with regard to the general limitation standard in final § 1033.421(a), limiting third parties to using covered data only as reasonably necessary for the provision of the product or service that the consumer requested ensures that consumers understand the scope of their authorization and retain control over their data. The CFPB is concerned, based on the current rulemaking record, that an exception to the secondary use prohibition for de-identified data would be inconsistent with the kind of meaningful consumer control that the final rule seeks to achieve, and might enable third parties to offer products and services that are primarily designed to accumulate large amounts of de-identified consumer data. Additionally, the CFPB notes that, as with identifiable covered data, the final rule does not prohibit third parties from using de-identified data as reasonably necessary to provide the consumer's requested product or service, or from seeking a separate authorization to use de-identified data for other purposes that the consumer may choose. Indeed, to the extent that covered data can be de-identified and still used to provide the product or service, the CFPB expects that third parties may take that step because it will provide a better means of safeguarding data.

Importantly, many of the beneficial purposes for which commenters seek to use de-identified data typically would not be secondary uses under the general limitation standard provided in § 1033.421(a). For example, § 1033.421(c) includes as an example that covered data—whether identifiable or de-identified— could be used as reasonably necessary to prevent fraud, service or process the consumer's requested product or service, and to improve the consumer's requested product or service. These examples of uses that are reasonably necessary to provide the consumer's requested product or service pursuant to § 1033.421(a) generally address the data uses described by commenters. For example, with appropriate safeguards pursuant to their third party obligations, third parties are generally permitted to use data, including de-identified data, to train a fraud detection algorithm or to improve the budgeting recommendation attribute of a personal financial management service.[115]

The CFPB acknowledges commenters' representations regarding the value of de-identified data for research purposes. Indeed, the CFPB uses de-identified data itself for research and market monitoring. But the use limitations in § 1033.421(a) and (c) operate in a particular context, where it is necessary to ensure that third parties that represent that they are acting on a specific consumer's behalf are actually doing so. Importantly, nothing prohibits a third party from seeking the consumer's separate authorization to use de-identified data for research purposes if that purpose is properly presented as an authorization for data access for a standalone product or service. Nonetheless, the CFPB recognizes that public interest research may present

[115] Additionally, as described elsewhere, the general standard to retain covered data as reasonably necessary would allow third parties to retain covered data used for these purposes for as long as reasonably necessary to locate the data and delete it. The CFPB is aware that it could be practically infeasible for third parties to delete data in certain circumstances, and as such, it would be consistent with the general limitation standard for the third parties to retain the data. In one such circumstance, for example, it might be practically infeasible for a third party using covered data in fraud prevention and product improvement models to extract from those models data no longer connected to a consumer who requests revocation.

unique considerations not developed in the current rulemaking record. Accordingly, the CFPB will consider whether a follow-on rulemaking would be appropriate to allow for public interest research uses of de-identified data outside of the general standard finalized in this rule.

The CFPB disagrees with commenters' assertions that the restrictions on secondary use would harm competition and therefore consumers by overly limiting potentially beneficial data uses. Under the final rule, third parties can use covered data as reasonably necessary to provide consumer-requested products and services, including uses that are reasonably necessary to improve those products and services. The CFPB expects that this will result in robust competition with respect to consumer-requested products and services. Further, the CFPB notes that the final rule does not restrict a third party's ability to obtain or use data in other ways unrelated to the final rule's data-access procedures, nor does the final rule prevent third parties from obtaining authorization from consumers to use covered data for additional products and services, including for research purposes. In addition, to the extent it is reasonably necessary to provide the consumer's requested product or service, third parties may use covered data as one input to the generation of new data that is not subject to the requirements of subpart D, including the limitations on secondary use (although other State and Federal laws may impose applicable restrictions).

For these same reasons, the CFPB also disagrees with comments suggesting that the rule, including not adopting the GLBA's privacy standard, creates an illogical or unfair distinction between data providers and third parties. Both data providers and third parties may use data that result from direct consumer relationships without adhering to the general limitation standard in § 1033.421(a), such as by using it as permitted under the GLBA and Regulation P, to the extent applicable. The final rule also does not treat covered data providers differently than other third

parties when they act as authorized third parties themselves—while they may use the data they generate in the course of providing their products or services in any manner allowable by law, they are still subject to the prohibition on secondary uses when accessing data from other data providers pursuant to the rule's procedures. The CFPB considers the final rule's approach to the use of generated data to be straightforward, but to the extent parties seek any additional guidance, the CFPB may publish responsive guidance as appropriate.

Accuracy (§ 1033.421(d))

Proposed § 1033.421(d) would have required third parties 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. Under the proposed rule, a third party would have flexibility to determine its policies and procedures in light of the size, nature, and complexity of its activities, but the third party would be required to periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness. The proposed rule provided two examples of elements in § 1033.421(d)(3) that third parties would have been required to consider when developing their policies and procedures regarding accuracy: (1) accepting covered data in the format required by the standards for developer interfaces in § 1033.311(b) and (2) addressing information provided by a consumer, data provider, or another third party regarding inaccuracies in the covered data. Finally, the proposed rule stated that 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.

The CFPB explained that proposed § 1033.421(d) would limit the scope of a third party's required policies and procedures to the accuracy of transmission—that is, receiving covered data

from a data provider and, if applicable, subsequently providing it to another third party. The CFPB provided several reasons for limiting this scope. First, existing Federal law already protects consumers against some of the most harmful inaccuracies in the use of financial data.[116] Second, the CFPB noted that most SBREFA comments addressing accuracy focused on transmission of data from data providers to third parties as the source of accuracy issues. In adopting a similar focus, proposed § 1033.421(d) reflected this feedback. Finally, the CFPB explained many third parties are small entities, and accuracy requirements covering all aspects of the collection, use, and provision of consumer data might be overly burdensome.

The CFPB sought comment on whether any additional elements bearing on the reasonableness of a third party's policies and procedures regarding accuracy should be included.

One Member of Congress expressed support for the proposed accuracy requirements. This commenter stated that inaccuracies would limit the ability of covered data to serve consumers and the financial system. On the other hand, some commenters opposed the inclusion of certain requirements. Some commenters believed that industry standards would be poorly suited to accuracy requirements. For example, a bank trade association stated that standardizing accuracy across the diverse universe of third parties may not be possible, given the broad array of interests.

Additionally, while not opposing the proposed requirement, a number of data provider and data provider trade association commenters recommended that the final rule do more to account for the fact that most third parties will receive data from data aggregators using proprietary formats rather than directly from data providers. Specifically, a few commenters

[116] For example, Regulation E protects consumers against unauthorized electronic fund transfers and other errors, and Regulation Z protects consumers against certain billing and servicing errors. *See* 12 CFR part 1005; 12 CFR part 1026.

recommended that the CFPB either prescribe a standardized format or remove the provision requiring third parties to consider accepting data in the format required for data providers' developer interfaces. One research organization commented that the CFPB might want to more clearly distinguish the obligations of third party data recipients and third party data aggregators.

Further, some third party commenters and one consumer advocate group commenter recommended the final rule contain a more robust dispute process. In particular, the consumer advocate group recommended a dispute process similar to that provided under the FCRA, wherein the consumer can dispute inaccuracies and require that a reasonable investigation is conducted.

For the reasons discussed herein, the CFPB is finalizing § 1033.421(d) as proposed, with one clarifying change to conform to the final rule's use of the term "consensus standard."

Accurate transmission of covered data is important for the effective functioning of the market for consumer-authorized data sharing. Inaccuracies in covered data impair third parties' ability to use that data for innovative purposes, undermining the benefits of data sharing for consumers. Accuracy standards also help ensure that authorized third parties are acting on behalf of consumers. Third parties that fail to take reasonable steps to ensure accuracy when receiving or transmitting covered data would not be acting in the interests of the consumers to whom the data relates. The specific arrangement that a third party makes to receive covered data affects the reasonableness of its policies and procedures regarding accuracy. For example, the CFPB understands that third parties frequently use data aggregators to obtain access to consumers' covered data. Such third parties should account for the involvement of a data aggregator by ensuring that their policies and procedures include measures to reduce inaccuracies that might be introduced by using an intermediary.

Standard-setting organizations can facilitate a comprehensive set of policies and procedures for accuracy that may be used by third parties throughout the consumer-authorized data sharing market. In particular, standard-setting organizations are likely to develop standards that are relevant to reasonable policies and procedures for accuracy—such as standardized data formats—that will increase the interoperability of the final rule. Further, recognized standard setters will need to consider input from both data providers and third parties, and as part of the balance attribute of § 1033.141(a), will specifically need to consider the input of small entity data providers. Accordingly, a recognized standard setter can—contrary to the suggestion of one commenter—issue consensus standards flexible enough to accommodate the wide array of third party data recipients.

Regarding comments concerning transmission of standardized formats, accepting data in the format in which it is transferred is relevant to ensuring accuracy. Section 1033.421(d)(3) does not preclude third parties from accepting covered data from a data aggregator in a standardized format. The flexibility provided by the policies and procedures allows the third party to accept covered data in a way that is best for the size and nature of the third party.

Additionally, CFPA section 1033(d) requires the CFPB to prescribe standards applicable to covered persons to promote the development and use of standardized formats for information. As discussed in more detail under § 1001.2(b) below, CFPA section 1002(15)(A)(vii) defines as a financial product or service "providing payments and other financial data processing to a consumer by any technological means" and data aggregators are therefore covered persons under

the CFPA.[117] The CFPB intends to monitor the market to evaluate whether data aggregators and authorized third parties are using standardized and machine-readable formats for covered data.

Regarding comments for a more robust dispute process, the CFPB has determined that forgoing overly prescriptive dispute requirements can facilitate consistency with robust accuracy requirements.[118] As the CFPB has noted, third parties are likely to be highly diverse in size and sophistication. The dispute requirement attempts to ensure that the burden of considering disputes is appropriate to the role that a third party played in the ecosystem. All third parties will need to consider "addressing information provided by a consumer, data provider, or another third party regarding inaccuracies in the covered data," but what is "reasonable" will depend on the size and sophistication of the third party. For example, data aggregators will likely have more extensive dispute processes than third parties that merely receive data. Further, the overall flexible nature of the policies and procedures accuracy requirement will allow third parties leverage existing systems for addressing disputes to the extent that such disputes also relate to the transfer of covered data.

The CFPB has determined that consumers will benefit from accuracy requirements for third parties. Third parties that fail to accurately receive data from a data provider, or fail to accurately provide data to another third party (when that is appropriate under the general limitation on data use), limit the effectiveness of the data access right fundamental to CFPA section 1033. Such inaccuracies also impair the development of an innovative, competitive market for alternative consumer financial products and services. Third party accuracy

[117] CFPA section 1002(4) defines "consumer" to include "an agent, trustee, or representative acting on behalf of" a consumer. Therefore, when a data aggregator provides financial data processing to an authorized third party, the aggregator is also necessarily providing financial data processing to a consumer.

[118] As discussed above in part IV.4, certain entities, such as data aggregators, may have dispute resolution obligations under other statutes, such as the FCRA. The analysis for this provision is limited to obligations arising under part 1033 and does not supplant other accuracy dispute requirements.

requirements also benefit third parties that rely on intermediaries to facilitate consumer-authorized access.

Data security (§ 1033.421(e))

Proposed § 1033.421(e)(1) would have required a third party to certify that it will apply to its systems for the collection, use, and retention of covered data an information security program that satisfies the applicable rules issued pursuant to section 501 of the GLBA (15 U.S.C. 6801). Under proposed § 1033.421(e)(2), if the third party is not subject to section 501 of the GLBA, the third party will apply to its systems for the collection, use, and retention of covered data the information security program required by the FTC's Standards for Safeguarding Customer Information, 16 CFR part 314. The CFPB preliminarily determined that the GLBA Safeguards Framework could be used by third parties to appropriately protect consumer-authorized financial data.

A range of commenters supported the use of the GLBA Safeguards Framework for third party data security. One bank commenter stated that the GLBA Safeguards Framework would ensure consistent data security standards for all ecosystem participants. Additionally, one consumer advocate group commenter said the proposed rule would close gaps in data security coverage. Another bank commenter stated that third parties should, at a minimum, follow the GLBA Safeguards Framework.

On the other hand, one third party commenter argued that the Safeguards Framework should not be applied to third parties, because compliance would be overly burdensome for third parties. Additionally, some commenters believed the final rule should add more specificity to the Safeguards requirements, for example, by creating a presumption of compliance for previously utilized standards, or consensus standards.

A number of bank commenters argued that the final rule should apply the same GLBA Safeguards Framework guidelines used by the Federal functional regulators[119] to supervise financial institutions. In particular, some data providers and trade associations for data providers stated that the FTC Safeguards rule was less prescriptive and not supported by regular supervision. Similarly, a few commenters requested that the final rule address liability by subjecting third parties to additional data security obligations, such as the FFIEC Information Technology Examination Handbook because, they said, it was more detailed than the FTC Safeguards Rule.

Additionally, one third party merchant commenter and one third party commenter argued that the final rule should not require third parties that are merchants to certify to follow the GLBA framework when they use consumer-permissioned data to facilitate payments for services provided by the merchant. These commenters' concern was threefold. First, the commenters argued that the proposed rule was inconsistent with the CFPA's limits on the CFPB's authority with respect to merchants. Second, the commenters stated that merchants are already subject to data security requirements under the National Automated Clearing House Association (NACHA) and the payment card industry data security standards (PCI DSS), and, given these previous compliance obligations, adding the safeguards condition would be overly burdensome for the merchant third party. Finally, the commenters stated that, under the proposed rule, merchants could be incentivized to avoid GLBA Safeguards Rule standards by asking the consumer to go around the open banking transaction, for example, by requiring the consumer to type in their ACH account and routing number, or by asking the consumer for a payment card rather than using an open finance application.

[119] The term "functional regulators" is the term that the GLBA uses to identify applicable agencies.

For the reasons discussed herein, the CFPB is finalizing § 1033.421(e) as proposed. Final § 1033.421(e)(1) requires a third party to apply to its systems for the collection, use, and retention of covered data an information security program that satisfies the applicable rules issued pursuant to section 501 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801). Under § 1033.421(e)(2), if the third party is not subject to section 501 of the Gramm-Leach-Bliley Act, the third party will apply to its systems for the collection, use, and retention of covered data the information security program required by the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 CFR part 314.

Requiring third parties to certify that they will comply with the GLBA Safeguards Framework will appropriately protect covered data. The rule's requirement for third parties to certify that they will follow the GLBA Safeguards Framework ensures consistency in protection as covered data moves from a data provider to one or more third parties because all or substantially all data providers are already subject to the GLBA Safeguards Framework,[120] most likely the Interagency Guidelines Establishing Information Security Standards issued by the Federal functional regulators.

The CFPB declines to include greater specificity in the data security certification for third parties, as requested by some commenters. Regarding comments requesting incorporation of industry standards into third party data security provisions, the CFPB notes that changing the security framework beyond the proposed approach would create a new, CFPA section 1033-specific data security standard, which could add complexity for third parties. The CFPB has

[120] Section 501 of the GLBA (15 U.S.C. 6801) applies to financial institutions, which are defined as companies that offer consumers financial products or services like loans, financial or investment advice, or insurance.

determined that by not incorporating industry standards or overly prescriptive standards relating specifically to data security, the rule better facilitates compliance with CFPA section 1033.

Regarding comments on the inadequacy of the FTC Safeguards Rule compared to the Safeguards Guidelines, for reasons stated in the proposed rule, the CFPB has determined the FTC Safeguards Rule provides adequate protection. The commenters failed to engage with the proposed rule's explanation that the FTC's Safeguards Rule includes slightly more prescriptive requirements, such as encryption, for certain elements, because the Safeguards Rule must be usable by a financial institution to determine appropriate data security measures without regular interaction with an examiner from a supervising agency. Additionally, concerning third party liability, the CFPB finds that the final rule's data security requirements will help protect against data breaches and any ensuing losses that third parties or data providers might suffer.

The CFPB has determined merchant third parties that are authorized third parties under the rule should be required to certify to comply with the same data security obligations as other third parties. Although merchant commenters expressed concern that merchants are already subject to data security requirements through NACHA and PCI rules, the CFPB has determined the relative similarities between these rules and the FTC Safeguards Rule suggests that the burden imposed on the merchants by the final rule would be minor. The FTC Safeguards Rule requires financial institutions to design an information security program that addresses several elements, including designating a qualified individual, performing a risk assessment, implementing controls such as encryption and multi-factor authentication, and testing or monitoring the effectiveness of the program's controls. Similarly, NACHA and PCI rules requires covered financial institutions to develop, implement, and maintain an information

security program with administrative, technical, and physical safeguards designed to protect customer information.

Further, contrary to one merchant commenter's concern with what it felt was a one-size-fits-all approach in the proposed rule, the flexibility of the Safeguards Rule would allow for some discretion in how the merchant third parties structure their data security systems. Additionally, treating NACHA or PCI standards as sufficient for purposes of a third party's data security certification would allow a private entity to determine the substance of the final rule's data security standards. This approach creates a risk that future NACHA or PCI standards might diverge from the CFPB's views about the proper data security obligations for authorized third parties.

Regarding comments stating that the CFPB does not have the authority over merchant third parties to require those third parties to certify to comply with the FTC Safeguards rule, the CFPB notes that the certification requirement in § 1033.421(e), for merchants and all third parties, is a condition to access covered data and not a freestanding requirement.

Provision of covered data to other third parties (§ 1033.421(f))

The CFPB proposed in § 1033.421(f) to require a third party to certify that, before providing covered data to another third party, it will require that other third party by contract to comply with certain obligations. The proposed rule noted that, in some circumstances, third parties that are authorized to access covered data from a data provider on behalf of a consumer would need to share that data with another third party. The authorized third party's ability to share covered data would be limited by the conditions in proposed § 1033.421(a) and (c), under which the authorized third party would limit its use of covered data, including sharing data with other third parties, to what is reasonably necessary to provide the consumer's requested product

or service. Subject to that limitation, the authorized third party would be permitted to provide the data to another third party.

The CFPB proposed that the consumer protections provided by the third party obligations in proposed § 1033.421 generally would apply when the covered data are provided by the authorized third party to another third party. The CFPB noted that, otherwise, the third party that receives the data from the authorized third party would not be subject to, for example, the limitations on use or the requirements for data privacy and data security that apply to the authorized third party, and the consumer would lose these important protections for the covered data, which ensure that data are used on their behalf.

Accordingly, the CFPB proposed in § 1033.421(f) that, before providing the covered data to another third party, the authorized third party would certify that it will require the other third party by contract to comply with the third party obligations in proposed § 1033.421(a) through (g) and the condition in proposed § 1033.421(h)(3), upon receipt of the notice described in proposed § 1033.421(h)(2). Proposed § 1033.421(f) stated that any provision of covered data to another third party would be subject to the restriction in proposed § 1033.421(c), which specifies that provision of data to other third parties is a type of use of covered data that would be limited by proposed § 1033.421(a) to what is reasonably necessary to provide the consumer's requested product or service requested. Proposed § 1033.421(f) did not require the authorized third party to certify that it will bind the other third party by contract to comply with all of the third party obligations in proposed § 1033.421. The CFPB preliminarily determined that certain of the third party obligations would be of limited applicability to the other third party, including the obligation to provide certain information to the consumer in proposed § 1033.421(g) and the revocation obligation in proposed § 1033.421(h). The CFPB requested comment on whether the

approach in proposed § 1033.421(f) would provide sufficient protection to consumers and their covered data when an authorized third party provides that data to another third party. The CFPB also requested comment on which third party obligations in proposed § 1033.421 should be included in this approach.

A number of commenters addressed the proposed approach in § 1033.421(f). A bank trade association commenter and a trade association representing nonbank entities both supported the proposed rule's approach to applying third party obligations when third parties provide covered data to downstream parties. Other commenters, including a bank trade association, a bank, and a consumer advocate, maintained that the proposed approach in § 1033.421(f) would not provide sufficient protections for consumers' covered data when an authorized third party provided that data to downstream parties. The bank and bank trade association commenters and the bank commenter stated that the proposed approach of requiring the authorized third party to certify that it will include contractual provisions obligating downstream parties to comply with certain obligations in proposed § 1033.421 would be insufficient and that the rule should impose those obligations directly on downstream parties. The trade association commenter recommended that, at a minimum, the rule should provide that, in addition to including contractual provisions requiring a downstream party to comply with the obligations, the authorized party must also ensure that the downstream parties comply with the obligations. The bank trade association commenter and a bank commenter also recommended that the rule should require the authorized third party to disclose to the consumer and the data provider which other third parties will be provided with the covered data. The bank trade association commenter stated that disclosing this information would provide consumers with

transparency and control over their data and would allow data providers to conduct risk assessments of downstream parties.

Some commenters, including a bank, a bank trade association, and a consumer advocate, recommended that the rule clarify when an authorized third party may share covered data with a downstream party. They noted that an authorized third party would be permitted to access covered data only for the purpose of providing the consumer's requested product or service, so they stated that it is not clear when it would be permissible for the authorized third party to share the covered data with additional third parties. A research institute commenter stated that proposed § 1033.421(f) would not appear to be flexible enough to permit sharing with a downstream third party when the authorized third party accesses the covered data for certain products that involve the sharing of covered data. For example, the research institute commenter stated that it was not clear if the proposed approach would permit an authorized third party to access covered data to identify rent, cell phone, and utility payments and share that information by reporting those payments to CRAs to help build the consumer's credit.

For the reasons discussed herein, the CFPB is adopting § 1033.421(f) as proposed with two minor changes. As finalized, § 1033.421(f) provides that, before providing covered data to another third party, subject to the limitation described in § 1033.421(a) and (c), the third party must certify that it will require the other third party by contract to comply with the third party obligations in § 1033.421(a) through (f) and the condition in § 1033.421(i) upon receipt of the notice described § 1033.421(h)(2).

Under the proposed rule, third parties also would have been required to certify that they would require downstream parties to comply with the provisions in § 1033.421(g) (related to keeping consumers informed). However, the provisions in § 1033.421(g) would be of limited

relevance for downstream parties and the CFPB concludes that an authorized third party therefore should not be required to certify that it will include them in contracts with downstream parties with which it will share covered data. Section 1033.421(g)(1) requires a third party to provide the consumer with a copy of the authorization disclosure. The downstream third party would be receiving the covered data for the purpose of providing the product or service requested by the consumer from the authorized third party, and the authorized third party, not the downstream party would have provided the authorization disclosure to the consumer. Section 1033.421(g)(2) also requires a third party to provide contact information that enables a consumer to receive answers to questions about the third party's access to the consumer's covered data. The authorized third party, not a downstream party, is more likely to have a relationship with the consumer and the consumer is more likely to attempt to contact the authorized third party with questions about access to the consumer's covered data. Section 1033.421(g)(3) requires the third party to establish and maintain reasonable policies and procedures to ensure that the third party, upon request, provides certain information to the consumer. Again, the consumer is more likely to contact the authorized third party to obtain information and the information listed in § 1033.421(g)(3) is primarily information possessed by the authorized third party. Accordingly, the final rule does not require an authorized third party to include the obligations in § 1033.421(g) in contractual provisions with downstream parties. In addition, the final rule changes the reference from § 1033.421(h)(3) to § 1033.421(i) because, as described below, the final rule includes a new § 1033.421(i) that includes provisions from proposed § 1033.421(b)(4) and (h)(3).

The CFPB has determined that requiring a third party to certify that it will include contract provisions requiring downstream parties to abide by the specified obligations will

provide sufficient protections, including protections that impose limitations on use and requirements for data security. As discussed above in connection with the authorization procedures in § 1033.401, requiring a third party to certify that it will include contractual provisions requiring downstream parties to abide by the specified obligations will provide sufficient protection. If a downstream party breaches the obligation, the CFPB could enforce those obligations using its authority to prevent unfair, deceptive, or abusive acts or practices, and other regulators, the consumer, and the data provider also may be able to enforce those provisions.

The CFPB has concluded that further clarification of when an authorized third party may share covered data with downstream parties is not necessary. Section 1033.421(f) specifically references the limitations in § 1033.421(a) and (c), so the authorized third party is able to share data with other third parties only as reasonably necessary to provide the product or service requested by the consumer from the authorized third party. Accordingly, downstream parties will be able to use the data only to assist the authorized third party with providing the requested product or service and not for their own purposes. The CFPB also has determined that the approach in § 1033.421(f) is sufficiently flexible to accommodate products like those suggested by the research institute commenter for which sharing of data is part of the product. Sharing the data in those circumstances would be reasonably necessary to provide the product requested by the consumer.

The CFPB declines to require that the authorized third party certify that it will disclose the identity of any third parties with which it will share the consumer's covered data. With respect to data aggregators, § 1033.431(b) requires the authorization disclosure to include the name of any data aggregator that will assist the third party seeking authorization with accessing

covered data and a brief description of the services the data provider will provide. However, at the time of the authorization, the third party seeking authorization may not know if it will be sharing covered data with other third parties and, if it will, the identity of those third parties. Moreover, the limitations in § 1033.421(a) and (c) restrict the circumstances in which an authorized third party is permitted to share covered data with other third parties. Finally, a consumer that wants to obtain additional information from the authorized third party about such data sharing may do so, as provided in § 1033.421(g). Accordingly, the CFPB has determined that it is not necessary to provide information during authorization about sharing covered data with downstream parties.

As noted above, a bank trade association recommended that § 1033.421(f) require the authorized third party to certify that it also will ensure that any downstream parties that they provide with covered data are abiding by their contractual obligations. The CFPB expects that, in addition to certifying that they will include contract provisions obligating downstream parties with which they share data to comply with certain obligations, authorized third parties will take reasonable steps to ensure that those downstream parties are complying with those obligations. Authorized third parties are permitted to share covered data with downstream parties only as reasonably necessary to provide the consumer's requested product or service. The CFPB expects that authorized third parties will, in the interest of maintaining relationships with consumers and avoiding potential liability for violating their own certifications to consumers, including the certification that covered data will only be collected, used, and retained as reasonably necessary to provide the consumer's requested product or service, perform due diligence in determining which downstream parties they select to assist in providing the consumer's requested product or service and take reasonable steps to monitor those downstream parties.

Ensuring consumers are informed (§ 1033.421(g))

The CFPB proposed in § 1033.421(g) to require a third party to certify that it agrees to certain obligations designed to ensure that consumers can obtain information about the third party's access to their data.

Under proposed § 1033.421(g)(1), a third party would have been required to certify that it would provide the consumer with a copy of the authorization disclosure that is signed or otherwise agreed to by the consumer and reflects the date of the consumer's signature or other written or electronic consent. Upon obtaining authorization to access covered data on the consumer's behalf, the third party would deliver a copy to the consumer or make it available in a location that is readily accessible to the consumer, such as the third party's interface. The proposed rule specified that, if the third party made the authorization disclosure available in such a location, the third party also would have been required to certify that it would ensure it is accessible to the consumer until the third party's access to the consumer's covered data terminates. The CFPB sought comment on whether this is the right time period. The CFPB proposed § 1033.421(g)(1) because it preliminarily determined that consumers would benefit from being able to access authorization disclosures they have previously signed. For example, the consumer may not recall which third parties are accessing their data, what data are being accessed, and for what reasons. Without this information, it would be difficult for a consumer to decide whether to continue authorizing data access.

Under proposed § 1033.421(g)(2), a third party would have been required to certify that it would 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. The proposal stated that a third party could satisfy proposed § 1033.421(g)(2) through its existing customer

service functions, provided that this function is equipped to handle the relevant questions. The CFPB proposed § 1033.421(g)(2) because it preliminarily determined that the consumer should be able to contact the third party to receive answers to questions about the third party's access to the consumer's covered data. The proposed rule stated that the authorization disclosure would contain a limited amount of information pursuant to proposed § 1033.411(b), so it may not address every question the consumer has about the third party's data access. The CFPB sought comment on additional requirements regarding the nature of the contact that the consumer can access through the contact information provided by the third party, such as whether the consumer must be able to access a human contact or whether the consumer must receive a response within a specified timeframe.

Under proposed § 1033.421(g)(3), third parties would have been required to certify that they would establish and maintain reasonable written policies and procedures designed to ensure that the third party provides to the consumer, upon request, the following information about the third party's access to the consumer's covered data: (1) categories of covered data collected; (2) reasons for collecting the covered data; (3) names of parties with which the covered data was shared; (4) reasons for sharing the covered data; (5) status of the third party's authorization; and (6) how the consumer can revoke the third party's authorization to access the consumer's covered data and verification the third party has adhered to requests for revocation. Proposed § 1033.421(g)(3) stated that the third party had flexibility to determine its policies and procedures in light of the size, nature, and complexity of its activities, and the third party would periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness. The CFPB proposed § 1033.421(g)(3) because it preliminarily determined that, at any time during the third party's access to the consumer's data, the consumer

should be able to obtain this information from the third party. The CFPB proposed to require a third party to certify that it would provide the names of parties with whom the covered data are shared because the CFPB preliminarily determined that this information would be valuable for consumers to know to protect their privacy, exercise control over which parties are accessing their covered data, and evaluate whether to continue sharing data with the third party. The CFPB proposed to require a third party to certify that it would provide information about the status of the third party's authorization because it may not be apparent to the consumer whether the third party's authorization is still active or whether the third party is currently collecting data.

With respect to the information about the categories of covered data the third party is collecting, the reasons for collecting the covered data, and information about how the consumer can revoke the third party's access to the consumer's data, the proposed rule stated that some consumers may want to obtain this information by contacting the third party. The CFPB preliminarily determined that it would be appropriate to require the third party to certify that it would provide this information on request given that the third party originally provided this information on the authorization disclosure. The CFPB sought comment on whether the list in proposed § 1033.421(g)(3) should be modified, including whether additional categories of information should be added.

The CFPB received a few comments on proposed § 1033.421(g). A bank trade association commenter, a Member of Congress, and a consumer advocate commenter supported the proposed rule's general approach to requiring third parties to keep consumers informed because it would allow consumers to make decisions with respect to their sensitive financial data.

The bank trade association commenter requested that the method for accessing this information be easy and intuitive and that information on the duration of data sharing be made available to consumers. The Congressmember's comment supported information about data security being made available to consumers.

A different bank trade association commenter requested that any separate data aggregator certification be available to the consumer upon request from either the third party or the data aggregator. A consumer advocate commenter requested more formal requirements for transparency into downstream data flows, detailing each onward transfer as well as the purposes of the transfer to allow consumers visibility and control on how financial information would get subsequently utilized. Another consumer advocate commenter and an individual commenter asserted that third parties should be required to provide information on how the third party makes decisions using data, including what data are used. A data provider commenter requested that the data provider name be made available on a platform such as a consumer revocation dashboard rather than on the authorization disclosure.

For the reasons described herein, the CFPB is finalizing § 1033.421(g) with modifications. First, the CFPB is finalizing in § 1033.421(g)(3)(vii) an additional requirement that the third party certify to maintain policies and procedures to provide to consumers, upon request, a copy of any data aggregator certification statement that was provided to the consumer separate from the authorization disclosure, pursuant to § 1033.431(c)(2). The CFPB is finalizing § 1033.421(g)(3)(vii) to ensure that consumers have access to the same information regardless of whether a data aggregator certification was included in the authorization disclosure or in a separate data aggregator certification. Second, the CFPB is modifying the language of proposed § 1033.421(g)(3)(iii) to specify that names of any parties with which covered data was shared

must be made available in a form that is readily understandable to consumers for consistency with the authorization disclosure. Third, the CFPB is modifying the language of proposed § 1033.421(g)(3)(iii) to better align with the requirements in §§ 1033.401(c) and 1033.411(a). Final § 1033.401(c) does not include language stating that a third party can obtain a consumer's express informed consent by having the consumer "otherwise agree" to the authorization disclosure. Finally, the final rule makes non-substantive changes to the language of proposed § 1033.421(g)(3).

The CFPB is not modifying its approach regarding downstream data flows or notification of sharing with downstream parties because the proposed rule required third parties to provide the "names of parties with which the covered data was shared." The CFPB is not adding a requirement to provide information about how the third party uses data to make decisions because doing so would be outside the intended scope of a provision regarding providing information about data access. Additionally, such information may be, in whole or in part, proprietary information. The CFPB is not modifying § 1033.421(c) to include the data provider's name or information about duration of data access because the consumer will have this information in the authorization disclosure. Finally, the CFPB is not adding a requirement to include information about data security because this information may be highly technical and is unlikely to be useful to consumers.

Revocation of authorization (§ 1033.421(h))

Proposed § 1033.421(h) included three components related to the third party's certification to provide the consumer with a mechanism to revoke the third party's authorization to access the consumer's covered data. These components are discussed below.

Provision of revocation method (§ 1033.421(h)(1))

Under proposed § 1033.421(h)(1), the third party would certify to provide the consumer with a mechanism to revoke the third party's authorization to access the consumer's covered data that is as easy to access and operate as the initial authorization. Proposed § 1033.421(h)(1) also stated that the third party would also ensure the consumer is not subject to costs or penalties for revoking the third party's authorization.

The proposed rule stated that the CFPB preliminarily determined that for the consumer's authorization for third party data access to be meaningful, consumers need to be able revoke that authorization at any time. The proposed rule also stated that a mechanism being as easy as the initial authorization would ensure third parties would not bury the revocation mechanism or otherwise obfuscate consumers' ability to utilize it. Additionally, the proposed rule stated that, for revocation of authorization to be free of cost or penalties to the consumer, consumers should be able to revoke their authorization to data access for purposes of one product or service but maintain that same third party's data access for purposes of another product or service. Therefore, as part of proposed § 1033.421(h)(1), third parties would certify to allow consumers to revoke consent to data access for a particular product or service and maintain consent to data access for any others.

Comments about this aspect of the proposed rule from a Member of Congress, consumer advocates, research organizations, trade associations for credit unions and banks, third parties, data aggregators, and individuals were generally supportive of the proposed approach to requiring third parties to provide consumers with a method to revoke third party authorizations to access covered data. Commenters' suggested amendments, clarifications, or additions to the proposed rule included: consumers' ability to revoke should be nonwaivable and the mechanism

should be provided "without friction or delay;" the mechanism should allow revocations at the granular level, including allowing consumers to expressly select the account for which authorization is revoked; the mechanism should allow the consumer to revoke authorization for any entity involved with the data sharing transaction; the final rule should specify a time limit by which third parties must notify other parties of the revocation request; and data aggregators should be required to provide consumers with a revocation request.

After considering comments, and for the reasons discussed herein, the CFPB is finalizing proposed § 1033.421(h)(1) without substantive change. The CFPB is making a non-substantive modification to change "mechanism to revoke" to "method to revoke" for consistency with the provision that allows data providers to provide a revocation method to consumers. As described above, some commenters suggested the CFPB should state that revocation is nonwaivable and should be provided without friction or delay, or should allow for more granular choices. The CFPB declines to make these changes because § 1033.421(h)(1) sufficiently ensures consumers may revoke third party authorizations at any point. Further, the CFPB has determined that third parties are in the best position to understand the covered data they need to collect to facilitate provision of a consumer's requested product or service. Offering consumers granular revocations might confuse consumers or frustrate the third parties' ability to provide that product or service.

The CFPB affirms that, for revocation of authorization to be free of cost or penalties to the consumer, consumers should be able to revoke their authorization to data access for purposes of one product or service but maintain that same third party's data access for purposes of another product or service they are receiving from the third party. In other words, third parties conditioning the provision of one product or service on the consumer providing consent to data access for another product or service is a cost or penalty on the consumer. Therefore, as part of

§ 1033.421(h)(1), third parties must certify that they will allow consumers to revoke consent to data access for a particular product or service and maintain consent to data access for any others.

For the consumer's authorization for third party data access to be meaningful, consumers need to be able revoke that authorization at any time. For this reason, § 1033.421(h)(1) is designed to ensure consumers can provide meaningful authorization to third party data access and can easily and effectively revoke that authorization whenever they choose. Ensuring the revocation method is as easy to access and operate as the initial authorization ensures third parties do not bury the revocation mechanism or otherwise obfuscate, block, or interfere with consumers' ability to utilize it.

Notice of revocation (§ 1033.421(h)(2))

Under proposed § 1033.421(h)(2), the third party would certify to notify the data provider, any data aggregator, and other third parties to whom it has provided the consumer's covered data when the third party receives a revocation request from the consumer. The CFPB proposed to require authorized third parties to certify that they will notify other third parties of the consumer's revocation to ensure that those third parties that receive covered data from the authorized third party are aware of the status of the consumer's authorization and can, accordingly, meet applicable certifications related to use and retention of that data. The CFPB also proposed in § 1033.421(h)(2) to require authorized third parties to notify data providers of the consumer's revocation to ensure data providers are aware of the status of the consumer's authorization.

For the reasons discussed herein, the CFPB is finalizing § 1033.421(h)(2) as proposed. As described above, some commenters suggested that the final rule specify a time limit by which third parties must notify other parties of the revocation request. The CFPB has considered these

comments but concludes that § 1033.421(h)(1) sufficiently addresses the timing of the third party's notice of consumer revocation to other third parties, since it requires such notification when the third party receives the consumer's revocation request.

Effect of revocation

Proposed § 1033.421(h)(3) would have required the third party to certify that, upon receipt of a consumer's revocation request or notice of a revocation request pursuant to proposed § 1033.331(e), the third party will (1) no longer collect covered data pursuant to the most recent authorization, and (2) no longer 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 under proposed § 1033.421(a). The CFPB is finalizing these provisions without substantive change in § 1033.421(i), discussed below. Comments regarding proposed § 1033.421(h)(3) are discussed in detail below related to § 1033.421(i).

Effects of maximum duration and revocation on collection, use, and retention (§ 1033.421(i))

Proposed rule

As described above, proposed § 1033.421(b)(4) and (h)(3) addressed the effects of maximum duration and receipt of a revocation notice on collection, use, and retention of consumers' covered data. With respect to the effect of maximum duration and revocation on use and retention, proposed § 1033.421(b)(4)(ii) and (h)(3)(ii) would have specified, consistent with the general limitation in proposed § 1033.421(a), that when the maximum durational period ends and the consumer does not provide a new authorization, or upon receipt of a consumer's revocation request or notice of a revocation request pursuant to proposed § 1033.331(e), the third

party may no longer use or retain covered data that was previously collected unless use or retention remains reasonably necessary to provide the consumer's requested product or service under proposed § 1033.421(a). The proposed rule stated that, in the current market, third parties use and retain consumer data for reasons unrelated to providing a consumer-requested product or service, including after a consumer no longer receives the product or service from the third party. The proposed rule further stated that such residual use and retention, which seldom occurs with consumer awareness, can result in significant privacy and security risks to consumers and can undermine the consumer's ability to control access to their covered data. Proposed § 1033.421(b)(4)(ii) and (h)(3)(ii) would address this concern by making clear that the general limitation on use and retention in proposed § 1033.421(a) applies to use and retention of covered data after a one-year maximum durational period ends and the consumer does not provide a new authorization, or when a consumer requests revocation pursuant to proposed § 1033.421(h) or § 1033.331(e).

The proposed rule stated that, while use and retention of covered data will not be reasonably necessary for most purposes after the third party's authorization ends, it may continue in some circumstances. The proposed rule provided the following examples for when use and retention might continue: a subpoena could require the retention, beyond the maximum period, of specific data collected in that period; meeting such legal requirements can continue to remain reasonably necessary even if only in connection with providing the product prior to the expiration of the maximum period. The proposed rule also stated that the consumer could provide a clear, affirmative indication 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. In that context, use and retention of some or all of the data could meet

the general standard in proposed § 1033.421(a) even as the consumer no longer makes use of the product in any manner that would require continued data collection.

The proposed rule explained that the CFPB preliminarily determined that proposed § 1033.421(b)(4)(ii) and (h)(3)(ii) would provide third parties with sufficient flexibility to address circumstances in which continued use or retention of previously collected data might be permitted under the general standard in proposed § 1033.421(a), while ensuring that consumer data are not used and retained in a manner that does not properly reflect the control afforded the consumer under that same general standard.

Comments received

Support for the standard in proposed § 1033.421(a) included support for the general limitation principles as they would apply to third party retention of covered data. For example, a Member of Congress, a third party, and a trade association for data providers supported the general standard as it applies to retention. The third party stated that data should not be retained except to fulfill the service requested, while the trade association said cybersecurity risks increase when third parties can accumulate and store data.

Feedback on this aspect of the proposed rule fell into various categories, most notably: (1) seeking an exception to, or variation of, the general limitation standard related to retention; (2) asserting that consumers should have a role in determining how long data are retained; (3) asserting that the general limitation standard and the proposed rule's explanation do not provide enough clarity as to when third parties must no longer retain covered data; and (4) asserting that the retention standard is too general and not strong enough.

Commenters who requested an exception or variation on the limitation standard in the context of retention, mostly trade associations for third parties and research organizations,

suggested that the proposed rule on retention is too restrictive. Commenters with this view stated that the final rule should allow retention of de-identified or pseudonymized data for specific purposes, like supplemental primary uses, public secondary uses, or research, or allow retention of historical data for some period so the product, service, or tool remains populated if a consumer reauthorizes shortly after the durational period expires. Commenters also stated that a restrictive retention limit would be harmful to beneficial products and services that rely on historical data, like cash-flow underwriting. A trade association for banks asked that the final rule allow third parties to retain data as long as necessary to defend themselves from consumer complaints. Finally, a research organization suggested the final rule should implement affirmative data deletion deadlines and require that data retention beyond three years be supported by documentation that the data continues to be reasonably necessary for the provision of the consumer's requested products or services, unless retention is required for compliance with other laws.

Commenters that suggested that consumers should have a role in determining how long data are retained—mostly trade associations for banks and research organizations—stated that consumers should be able to consent to how long data are retained or should be able to opt in to retention of de-identified data. The same commenters suggested that the proposed rule was too vague for consumers to understand what will be retained or for third parties to know how to comply. Some commenters in this category suggested finalizing an explicit requirement to delete upon the expiration of duration or when a consumer revokes.

Some commenters, including research organizations and trade associations for banks, asserted that the retention standard is too general and not strong enough. One commenter stated that the proposed rule would only discourage indefinite retention and that the final rule should be

more prohibitive. Another suggested the final rule should implement mandatory time periods by which third parties must delete all data.

Finally, one third party commenter asked that the final rule clarify what happens to "copied data" held by authorized third parties and data aggregators.

Final rule

For the reasons described herein, the CFPB is finalizing in § 1033.421(i) the provision related to the effect of maximum duration on collection, use, and retention in proposed § 1033.421(c)(4) and consumers' revocation requests in proposed § 1033.421(h)(3). As such, under § 1033.421(i), if a consumer does not provide a new authorization as described in § 1033.421(b)(3), or if a third party receives a revocation request as described in § 1033.421(h)(1) or notice of a consumer's revocation request as described in § 1033.331(e), a third party will: (1) no longer collect covered data pursuant to the most recent authorization; and (2) no longer 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 under § 1033.421(a).

With respect to § 1033.421(i)(1), the CFPB has determined that the general limitation in § 1033.421(a) will require third parties to stop collecting covered data when the maximum durational period ends and the consumer has not provided a new authorization or when the consumer requests revocation. In those circumstances, collection would no longer be reasonably necessary to provide the consumer's requested product or service. Ensuring that collection stops at these points affords consumers control over the collection of covered data.

With respect to § 1033.421(i)(2), the CFPB has determined that the general limitation in § 1033.421(a) will, in most circumstances, require the third party to no longer use or retain

covered data when the maximum durational period ends and the consumer has not provided a new authorization or when the consumer requests revocation. The consumer revoking third party authorization or not providing a new authorization after one year, all other things being equal, indicates that the existing authorization, without more, no longer supports use or retention of covered data that has been collected under its terms. However, specific circumstances may justify departure from this normal course and, consistent with the general standard in § 1033.421(a), allow continued use or retention of some or all previously collected covered data, even when collection of new covered data has stopped.[121]

As described above, one commenter asked that the final rule clarify what happens to "copied data" that third parties might have following revocation. The commenter did not elaborate on the meaning of "copied data," but assuming copied data refers to copies of covered data that third parties receive or make, the CFPB notes that the general limitation under § 1033.421(a) would apply and such copied data could only be used or retained as reasonably necessary to provide the consumer's requested product or service.

Additionally, as described related to § 1033.421(b), in unusual circumstances a data provider might provide a third party more data than the third party requested. This may result in the third party involuntarily collecting more data than is reasonably necessary to provide the consumer's requested product or service. The CFPB notes that, in those circumstances, the general limitation on use and retention in § 1033.421(a) would apply to that data. While use of that data would not be reasonably necessary to provide the consumer's requested product or

[121] A third party commenter suggested that the proposed rule contained a technical error that would not provide sufficient flexibility for third parties to retain previously collected data for permissible uses. However, as noted, the final rule contains flexibility when circumstances justify such continued retention.

service, the general limitation standard would allow third parties to retain covered data for as long as reasonably necessary to locate and delete that data.

Finally, as noted above in § 1033.421(b) regarding collection, when the third party receives information that indicates the consumer may no longer expect to receive the product or service, the third party should confirm collection of covered data remains reasonably necessary. In those circumstances, use and retention of covered data may no longer be reasonably necessary. The CFPB has determined that § 1033.421(i)(2) provides third parties with sufficient flexibility to address circumstances in which continued use or retention of previously collected data might be justified under the general limitation. The certification in § 1033.421(i)(2) also ensures that covered data are not used and retained in a manner that does not properly reflect the control afforded the consumer when they do not provide a new authorization after a maximum durational period has ended or when they request revocation.

5. Use of data aggregator (§ 1033.431)

The CFPB proposed certain requirements for the third party authorization procedures when a third party uses a data aggregator to assist with accessing covered data on behalf of a consumer. Currently, many third parties rely on data aggregators to assist with accessing and processing consumer financial data. The CFPB proposed in § 1033.431 to assign certain responsibilities for the authorization procedures and impose certain conditions on the third party and the data aggregator.

A number of commenters addressed how the rule generally should treat data aggregators. Several commenters, including bank and bank trade association commenters stated that the rule should impose strong limitations on data aggregators. One bank trade association commenter stated that data aggregators often possess far greater bargaining power than third parties, so they

can dictate terms, and that the final rule should provide that data aggregators are jointly and severally liable for issues that occur at the third party to which it is providing services. A bank commenter stated that the proposal underestimates the systemic risks posed by data aggregators, noting that they likely have more consumer data than the largest banks and will continue to control vast amounts of data after the rule takes effect. Another bank trade association commenter and a credit union commenter stated that data aggregator should face even more stringent controls on their use of covered data because consumers have no meaningful choice over the aggregator that is used. Two bank trade association commenters recommended that the rule prohibit data aggregators from using covered data for their own purposes. Several commenters, including bank and bank trade association commenters, maintained that the rule should impose obligations directly on data aggregators, stating that the CFPB should be responsible for enforcing those obligations, rather than relying on the certification-based approach and relying on authorized third parties, consumers or data providers to ensure that data aggregators comply with the obligations. Several commenters, including bank and bank trade association commenters, requested that the CFPB exercise supervisory authority over data aggregators to ensure that they comply with the rule.

For the reasons discussed herein, the CFPB is generally adopting the approach to data aggregators as proposed, with certain changes in § 1033.431(c) regarding data aggregator certification. Those provisions are described in more detail below.

As finalized, § 1033.431 imposes various obligations on data aggregators, including the requirement in § 1033.431(c) that data aggregators must certify to the consumer that they will comply with specified obligations. The CFPB declines to provide that data aggregators are jointly and severally liable for issues that occur at the third party to which the data aggregator is

providing services. Depending on the context, those issues could arise from conduct unrelated to the services provided by the data aggregator, so the CFPB has determined that generally imposing joint and several liability would not be appropriate. The rule does, however, require data aggregators to certify to the consumer that they will comply with specified obligations, and in the event that data aggregators breach those obligations, the CFPB can use its authority to prevent unfair, deceptive, or abusive acts or practices, as appropriate, to enforce those obligations against data aggregators. For the reasons discussed in part IV.D.2, the CFPB has determined that the certification-based approach is appropriate for third parties, including data aggregators, and declines to impose additional obligations on third parties in this rule.

As noted above, some commenters urged the CFPB to impose additional restrictions on data aggregator use of covered data. The obligations in § 1033.421(a) and (c) limit the circumstances in which third parties can collect, use and retain covered data, and data aggregators must certify to consumers that they will comply with those obligations. Among other things, the covered data can only be used as reasonably necessary to provide the product or service requested by the consumer from the authorized third party. Accordingly, these provisions will prevent a data aggregator from using the covered data for its own purposes, and the CFPB has determined that additional restrictions on data aggregator use of covered data are unnecessary. With respect to supervision of data aggregators, as discussed in part IV.5, the CFPB's supervisory authority is defined by the CFPA. The CFPB will continue to monitor the market, including by using its supervisory authority, and will consider whether additional rulemakings are appropriate to expand the scope of the CFPB's supervision with respect to part 1033.

Responsibility for authorization procedures (§ 1033.431(a))

The CFPB proposed in § 1033.431(a) to allow, but not require, a data aggregator to perform the third party authorization procedures on behalf of the third party. Proposed § 1033.431(a) also provided that the third party would remain responsible for compliance with the third party authorization procedures and that data aggregators would have to comply with the data aggregator certification requirements in proposed § 1033.431(c).

The CFPB preliminarily determined that the third party should be responsible for compliance with the third party authorization procedures. The CFPB noted that the third party is providing a product or service to the consumer and is likely to have the primary relationship with the consumer, so the consumer may be more comfortable receiving and responding to communications from the third party. The third party also likely would be more involved in using and retaining covered data and therefore may play a greater role than the data aggregator. Moreover, the data aggregator is assisting the third party in accessing covered data, so the CFPB preliminarily determined that the third party should be responsible for compliance with the third party authorization procedures.

The CFPB noted, however, that some third parties may want to rely on data aggregators to perform the authorization procedures on their behalf and that, in some circumstances, it may be more efficient for data aggregators to do so. Therefore, the CFPB proposed to allow, but not require, a data aggregator to perform the authorization procedures on behalf of a third party. The CFPB noted that if a data aggregator performs the authorization procedures on behalf of the third party, the consumer's authorization would grant authority to the third party to access covered data on behalf of the consumer. The third party would retain the flexibility to discontinue using the data aggregator or switch to a different aggregator.

Several commenters addressed how to allocate responsibility for the authorization procedures when a data aggregator is involved. Commenters including a bank, a bank trade association, and a nondepository entity all supported the proposed approach of assigning responsibility for the authorization procedures to the third party seeking authorization but permitting the data aggregator to perform the authorization procedures on behalf of the third party.

A number of commenters recommended that the CFPB revise or clarify how the authorization procedures can be performed when an authorized third party retains a data aggregator. A bank commenter stated that the CFPB should clarify which authorization procedures may be performed by a data aggregator and which ones must be performed by the authorized third party. The bank commenter stated that the authorized third party should be responsible for describing the product or service to the consumer and providing a certification statement. The bank commenter also urged the CFPB to clarify that the requested product or service is referring to the product or service offered by the authorized third party and not a product or service offered by the data aggregator. The bank commenter also stated that the CFPB should clarify that when a data aggregator performs the authorization procedures on behalf of the authorized third party, the authorized third party remains responsible for its own compliance with the specified obligations. The bank commenter also urged the CFPB to distinguish the data aggregator's role when it is acting as an intermediary on behalf of an authorized third party from when it is attempting to become an authorized third party. The bank commenter also recommended that when a data aggregator is acting on behalf of an authorized third party, the data aggregator must fulfill all of its obligations under the rule independent of other connections the data aggregator may have fulfilled for the same consumer on behalf of a different third party.

A credit union commenter recommended that the CFPB remove all references to data aggregators from the rule and instead require data aggregators to comply with all of the requirements of an authorized third party. A third party commenter stated that the rule should clarify that data aggregators may perform the authorization procedures on their own behalf when they are operating as authorized third parties. A research institute commenter stated that the rule should encourage data aggregators to take on additional roles and responsibilities to support open banking and provide better experiences to consumers. The research institute commenter urged the CFPB to clarify when data aggregators can become authorized third parties.

For the reasons discussed herein, the CFPB is adopting § 1033.431(a) as proposed. Section 1033.431(a) allows, but does not require, a data aggregator to perform the third party authorization procedures described in § 1033.401 on behalf of the third party seeking authorization under § 1033.401 to access covered data. Under § 1033.431(a), the third party seeking authorization remains responsible for compliance with the third party authorization procedures described in § 1033.401. Data aggregators must comply with the data aggregator certification requirements in § 1033.431(c).

As indicated in § 1033.431(a), the authorized third party remains responsible for complying with the authorization procedures, including certifying to the consumer that it will comply with the obligations in § 1033.421. However, the data aggregator may perform the certification procedures on behalf of the authorized third party. If the data aggregator performs the authorization procedures on behalf of the authorized third party, the data aggregator must complete the authorization procedures for the authorized third party and provide the authorization disclosure with the content required in § 1033.411(b). The data aggregator must also obtain the consumer's express informed consent for the authorized third party to access

covered data on behalf of the consumer as required in § 1033.401(c). As discussed below in connection with § 1033.431(c), the data aggregator must also certify that it will comply with the certification requirements specified in § 1033.431(c).

The CFPB recognizes that third parties may play different roles in different transactions. A third party may be a data aggregator in one transaction and an authorized third party in a different transaction. However, a third party cannot perform both roles in the same transaction. If a third party is serving as a data aggregator, it cannot collect, use, and retain the consumer's covered data for its own purposes. It is limited to accessing the information only as reasonably necessary for providing the product or service requested by the consumer from the authorized third party. When a data aggregator performs the authorization procedures on behalf of an authorized third party, those authorization procedures apply only to that authorized third party. If the data aggregator is assisting a second authorized third party in accessing covered data from the same consumer, the second authorized third party or the data aggregator acting on behalf of that second authorized third party must perform the authorization procedures separately for that second authorized third party.

The CFPB concludes that it is appropriate to identify and adopt specific provisions applicable for data aggregators separately from authorized third parties. Data aggregators perform a different role than authorized third parties, and the CFPB has determined that the rule should highlight that the authorized third party is responsible for obtaining the consumer's authorization to access the consumer's data.

Disclosure of the name of the aggregator (§ 1033.431(b))

The CFPB proposed in § 1033.431(b) to require that the authorization disclosure include the name of any data aggregator that will assist the third party seeking authorization under

proposed § 1033.401 with accessing covered data and a brief description of the services the data aggregator will provide. The proposed rule stated that, unlike other downstream parties that may access a consumer's covered data after a third party has completed the authorization procedures, a data aggregator is typically known to the third party at the time of authorization and a consumer may directly interact with a data aggregator when the data aggregator performs the authorization procedures on behalf of the third party. Therefore, the CFPB preliminarily determined that identifying and describing the services of a data aggregator would reduce consumer confusion and better equip consumers to provide informed consent when authorizing data access. The proposed rule requested comment on any obstacles to including a data aggregator's name in the authorization disclosure.

A consumer advocate commenter and a credit union commenter supported including information about the data aggregator in the authorization disclosure to provide sufficient transparency. The credit union commenter requested that both the legal and trade names of the data aggregator be included in the authorization disclosure.

For the reasons discussed herein, the CFPB is finalizing § 1033.431(b) as proposed. Including the data aggregator name and a description of the data aggregator's services in the authorization disclosure provides consumers with a key term of access that may reduce consumer confusion and better equip consumers to provide informed consent. Commenters did not raise concerns with this approach.

The CFPB is not modifying § 1033.431(b) to require the inclusion of a data aggregator's legal and trade names, as suggested by one commenter. The final rule does not require authorized third parties to include their own legal and trade names, and it would be inconsistent to require authorized third parties to provide the legal and trade names of data aggregators.

Additionally, including multiple names for a single data aggregator would make the authorization disclosure longer, and it is not clear that this added information would make a significant impact on a consumer's ability to identify the data aggregator. Finally, as discussed above, the CFPB is finalizing a requirement that the name of the data aggregator must be "readily understandable" to consumers, which will help ensure that consumers are able to identify the data aggregator.

Aggregator certification (§ 1033.431(c))

The CFPB proposed in § 1033.431(c) that when a third party seeking authorization under § 1033.401 will use a data aggregator to assist with accessing covered data on behalf of a consumer, the data aggregator must certify to the consumer that it agrees to the conditions on accessing the consumer's data in proposed § 1033.421(a) through (f) and the condition in proposed § 1033.421(h)(3) upon receipt of the notice described in proposed § 1033.421(h)(2) before accessing the consumer's data. However, the data aggregator would not have been required to certify that it would provide a revocation method or certify to the requirements related to ensuring consumers informed.

The CFPB explained it was proposing to require data aggregators to certify that they agree to these conditions because, when a third party uses a data aggregator, the aggregator may play a significant role in accessing the consumer's data. Data aggregators may, among other things, process the consumer's login credentials, obtain the consumer's data from the data provider, and transmit the consumer's data to the third party. The CFPB stated that, if data aggregators were not required to agree to these conditions, there could be a significant gap in the protections afforded to consumers.

In addition, as with the third party's certification statement, the CFPB wanted the consumer to receive a clear statement of the conditions that the data aggregator must follow. The certification statement to the consumer would help consumers, the CFPB, and other regulators to enforce the obligations to which data aggregators would be required to certify. The CFPB stated that these considerations are equally applicable to data aggregators that are retained by the authorized third party after the consumer has completed the authorization procedures, so proposed § 1033.431(c) would require those data aggregators to also provide a certification to the consumer.

The CFPB also proposed in § 1033.431(c) that any data aggregator that is retained by the authorized third party after the consumer has completed the authorization procedures must also satisfy this aggregator certification requirement. For this requirement to be satisfied, either (1) the third party seeking authorization under proposed § 1033.401 must include this aggregator certification in the authorization disclosure described in proposed § 1033.411 it provides the consumer, or (2) the data aggregator must provide to the consumer a separate certification. The CFPB stated that, for example, the aggregator certification requirement in proposed § 1033.431(c) would be satisfied where the authorization disclosure includes a statement that both the third party and the data aggregator agree to the applicable third party obligations described in proposed § 1033.421. The CFPB further stated that this requirement would also be satisfied where the data aggregator provides the certification to the consumer in a separate communication. When a data aggregator is retained by the authorized third party after the consumer has completed the authorization procedures, proposed § 1033.431(c) would not require the consumer to receive a new authorization disclosure or provide consent. The CFPB sought

comment on whether to include formatting or language access requirements for an aggregator certification that is provided in a separate communication from the authorization disclosure.

Regarding the format of the separate data aggregator certification, a consumer advocate commenter requested that the CFPB include the following formatting and language access requirements in the final rule: require model forms, including mobile-friendly versions; require provision in any language that the authorization was required to be provided in; set a maximum reading level; and specify timing.

Regarding content of the data aggregator certification, several bank commenters and a consumer advocate commenter requested that data aggregators provide a revocation mechanism to ensure that consumers have the ability to revoke authorization with any entity involved in the data sharing transaction. Several bank commenters and a consumer advocate commenter also requested that data aggregators comply with the requirements related to ensuring consumers are informed in § 1033.421(g) given data aggregators' significant involvement in the handling of consumer data. These commenters stated that, because of data aggregators' significant role, consumers may want to contact data aggregators with questions about the services the data aggregator provides.

For the reasons discussed herein, the CFPB is finalizing § 1033.431(c) with certain modifications. The CFPB is finalizing the required content of the aggregator certification in the introductory text of § 1033.431(c) with non-substantive changes. Consistent with the proposal, the CFPB is not requiring data aggregators to certify to comply with § 1033.421(g) (the certification related to ensuring consumers are informed) because this would require the data aggregator to significantly increase coordination with the third party, such as by finding out with which downstream parties the third party has shared the consumer's covered data. This would

result in little benefit to consumers because consumers would already receive this information from third parties. Requiring data aggregators to certify to comply with the § 1033.421(g) requirements could also result in consumers receiving unwanted duplicative information, such as two copies of the authorization disclosure (one from the third party and one from the data aggregator). The CFPB is also not requiring a data aggregator to certify that it will provide consumers with a revocation mechanism because a data aggregator would potentially have to create a consumer-facing interface to create a revocation mechanism which is not otherwise required by final rule. However, data aggregators are permitted to provide a revocation mechanism if they choose to do so.

The final rule includes non-substantive changes to the introductory text to § 1033.431(c), including, in the list of provisions that must be included in the certification, changing the reference from § 1033.421(h)(3) to § 1033.421(i) because, as described above, the final rule includes a new § 1033.421(i) that includes provisions from proposed § 1033.421(b)(4) and (h)(3). The introductory text of proposed § 1033.431(c) stated that any data aggregator that is retained by the authorized third party after the consumer has completed the authorization procedures must also satisfy this requirement. This substantive requirement is moved to final § 1033.431(c)(2) to clarify that the certification for a data aggregator retained by an authorized third party after the consumer has completed the authorization procedures would have to be provided pursuant to § 1033.431(c)(2).

The CFPB is finalizing as proposed § 1033.431(c)(1), requiring that if the data aggregator does not provide its certification to the consumer as set forth in § 1033.431(c)(2), the third party seeking authorization under § 1033.401 must include the data aggregator's certification in the authorization disclosure described in § 1033.411.

Final § 1033.431(c)(2) provides that, consistent with the general requirements for the authorization disclosure, the data aggregator must provide its certification to the consumer, electronically or in writing, separate from the authorization disclosure. As is also consistent with the requirements for the authorization disclosure and for the reasons explained above in part IV.D.3 in connection with the requirements for the authorization disclosure, the certification must be in the same language as the authorization disclosure and must be clear, conspicuous, and segregated from other material. The final rule does not require model forms, reading level, or timing requirements for the aggregator certification, consistent with the final rule's approach to the authorization disclosure in § 1033.411(a), described above.

Final § 1033.431(c)(2) also provides that the name of any data aggregator in the certification must be readily understandable to the consumer. As explained above in the discussion of § 1033.411(a), this requirement will help ensure that consumers are able to easily identify the entities in the certification. As noted above, final § 1033.431(c)(2) also provides that if, after the consumer has completed the authorization procedures, the authorized third party retains a data aggregator to assist with accessing covered data on behalf of the consumer, this data aggregator must provide its certification in accordance with § 1033.431(c)(2).

6. Policies and procedures for third party record retention (§ 1033.441)

Proposed § 1033.441(a) would have required a third party that is a covered person or service provider, as defined in 12 U.S.C. 5481(6) and (26), to establish and maintain written policies and procedures that are reasonably designed to ensure retention of records that are evidence of compliance with the requirements of proposed subpart D. Under proposed § 1033.441(b), records required under proposed § 1033.441(a) would have to be retained for a

reasonable period of time, not less than three years after a third party obtains the consumer's most recent authorization under proposed § 1033.401(a).

Proposed § 1033.441(b) based the retention period on the date of the consumer's most recent authorization because that event would determine when compliance with proposed subpart D would begin to be required. The CFPB explained that the minimum three-year period should be sufficient for the CFPB and others to evaluate compliance with respect to any given authorization because proposed § 1033.421(b)(3) would require third parties to obtain a new authorization each year. The CFPB clarified that proposed § 1033.421(b)(4) and (h)(3) were not designed to impact the requirement for a third party to maintain policies and procedures to retain records for a reasonable period proposed in § 1033.441, noting that proposed § 1033.441 covered records that evidence compliance with proposed subpart D. In contrast, proposed § 1033.421(b)(4) and (h)(3) covered data collected from data providers to provide a requested product or service.

Under proposed § 1033.441(c), a third party covered under proposed § 1033.441(a) would have flexibility to determine its policies and procedures in light of the size, nature, and complexity of its activities. The CFPB explained that this flexibility would help third parties avoid conflicts with other legal obligations (including other record retention and data security obligations), manage data security risks, and minimize unnecessary impacts.

To mitigate the risk that the flexibility of proposed § 1033.441(c) might result in the absence of critical evidence, proposed § 1033.441(e)(1) and (2) would have identified examples of records that would need to be retained. Specifically, proposed § 1033.441(e) would have provided that records retained pursuant to policies and procedures required under proposed § 1033.441 must include, without limitation (1) a copy of the authorization disclosure that is

signed or otherwise agreed to by the consumer and reflects the date of the consumer's signature or other written or electronic consent and a record of actions taken by the consumer, including actions taken through a data provider, to revoke the third party's authorization; and (2) with respect to a data aggregator covered under proposed § 1033.441(a), a copy of any data aggregator certification statement provided to the consumer separate from the authorization disclosure pursuant to proposed § 1033.431(c)(2).

Proposed § 1033.441(d) would have required a third party covered under proposed § 1033.441(a) to periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness to evidence compliance with the requirements of proposed subpart D.

The CFPB explained that the flexible policies and procedures approach of proposed § 1033.441 would be consistent with the SBREFA Panel's recommendation that the CFPB evaluate record retention requirements for consistency with other requirements and the avoidance of unnecessary data security risks, while still ensuring all evidence of compliance by a third party is retained.

The CFPB requested comment on the proposed length of the retention period and whether it should be based on another event, such as the termination of a third party's authorization or a third party's request for information from a data provider. The CFPB also requested comment on whether the final rule should identify other examples of records to be retained. Additionally, the CFPB requested comment on whether additional guidance was needed on the potential intersections of the record retention requirements in proposed § 1033.441 and limitations on retention in proposed § 1033.421(b)(4) and (h)(3).

Commenters generally supported the proposed requirement for third parties to establish and maintain policies and procedures reasonably designed to ensure retention of records that evidence compliance with proposed subpart D. One bank industry group supported measuring the retention period beginning at the time the third party obtains the consumer's most recent authorization. Another such group supported the three-year record retention requirement. On the other hand, some bank industry commenters suggested that the retention period should be two years. These commenters stated that this would make the retention requirement consistent with similar requirements to which data providers are already subject under Regulation E and Regulation Z. Further, they stated that the additional year does not pose any benefit to consumers and that the additional length to retain presents unnecessary security risks.

For the reasons discussed herein, the CFPB is finalizing § 1033.441(a) through (d) as proposed. The CFPB is finalizing § 1033.441(e) generally as proposed, with minor non-substantive edits for consistency with other revisions elsewhere in the final rule. Specifically, records retained pursuant to policies and procedures required under § 1033.441 must include, without limitation: (1) a copy of the authorization disclosure that is signed by the consumer electronically or in writing and reflects the date of the consumer's signature and a record of actions taken by the consumer, including actions taken through a data provider or another third party, to revoke the third party's authorization; and (2) with respect to a data aggregator covered under § 1033.441(a), a copy of any data aggregator certification statement that was provided to the consumer pursuant to § 1033.431(c)(2). The CFPB expects that in order to ensure accuracy, record integrity, and to preserve the ability to access the signed authorization disclosure, the authorization disclosure and the electronic signature establishing consumer consent cannot as a matter of regular course be provided orally and still satisfy all of the final rule's requirements.

Section 1033.441 is authorized under CFPA section 1022(b)(1) because it will enable the CFPB and others to evaluate a third party's compliance with subpart D and would prevent evasion. To the extent that § 1033.441 applies to CFPB-supervised nondepository covered persons, it is additionally authorized by CFPA section 1024(b)(7) because it will facilitate supervision of such persons and enable the CFPB to assess and detect risks to consumers.

The CFPB determines that the three-year length of the retention requirement in § 1033.441(b) is appropriate and the CFPB declines to align it with the retention requirements in Regulation E and Regulation Z, as requested by some commenters. The retention requirements under Regulation E and Regulation Z are substantively different from those in § 1033.441. Records required under Regulation E and Regulation Z relate to regulated entities' disclosures to consumers pertaining to electronic fund transfers and consumer credit, respectively. Such disclosures to individual consumers are likely to be stale after a period of two years. Three years of records contemplated by § 1033.441 will allow for analysis of a third party's compliance with part 1033, including patterns in third party actions in requesting access to a data provider's interface and the authorizing consumer's data over time. Moreover, based on the CFPB's supervisory and enforcement experience, a three-year retention period is an appropriate amount of time to enable the CFPB and other enforcement agencies to examine or conduct enforcement investigations.

12 CFR Part 1001

Providing financial data processing products or services (§ 1001.2(b))

Proposed § 1001.2(b) would have defined providing 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, as a financial

product or service under the CFPA. The proposed provision included certain limited exclusions. After considering public comments, the CFPB is finalizing the provision as proposed.

Statutory framework

Under CFPA section 1002(15)(A)(xi)(II), the CFPB may issue a regulation to define as a financial product or service "such other financial product or service" that the CFPB finds 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." The CFPB is issuing § 1001.2(b) pursuant to this authority. In turn, under the CFPA, a financial product or service under § 1001.2(b) would qualify as a "consumer financial product or service" under CFPA section 1002(5)(A) if it "is offered or provided for use by consumers primarily for personal, family, or household purposes."

As the CFPB explained in the proposal, the activities in § 1001.2(b) would have already been within scope of the CFPA's definition of financial product or service. Specifically, CFPA section 1002(15)(A)(vii) defines as a financial product or service "providing payments and other financial data processing to a consumer by any technological means." The language of this provision extends beyond payment processing to broadly include other forms of financial data processing. Accordingly, consumers already receive the protections of the CFPA when entities process their potentially sensitive data, whether payments or any other category of financial or banking data.[122] On this issue, a trade association of the nonbank money services industry submitted a comment agreeing that the activities in § 1001.2(b) are already within the scope of

[122] Many of these activities could also fall within other categories of financial product or service. *E.g.*, CFPA section 1002(15)(A)(ix), 12 U.S.C. 5481(15)(A)(ix) ("collecting, analyzing, maintaining, or providing consumer report information or other account information" under specified circumstances).

the CFPA. Consistent with the proposed rule, the CFPB is using its rulemaking authority under CFPA section 1002(15)(A)(xi)(II) to provide even greater certainty regarding CFPA coverage.[123]

Overview of § 1001.2(b)

By conferring authority on the CFPB to define additional financial products or services, the CFPA accounts for the possibility that the enumerated list of financial products and services in CFPA section 1002(15)(A)(i) through (x) may not completely capture the markets for financial products or services that are significant for consumers, especially as market developments lead to emerging concerns for consumers. As already noted, the final rule has the potential to expand access to personal financial data and subject such data to a wider variety of data processing activities. The CFPB is adding to the definition of financial product or service the category of "providing financial data processing products or services" to ensure that activities involving consumers' potentially sensitive personal financial information are subject to the CFPA and its prohibition on unfair, deceptive, or abusive acts or practices to the full extent authorized by Congress.[124] The definition includes examples to illustrate the activities that fall within the term financial data processing. Section 1001.2(b) clarifies that the financial data processing products or services that are covered by the definition could be offered either alone or in connection with another financial or nonfinancial product or service, and so it does not cease to be covered simply because it is offered in connection with the latter.[125]

[123] Accordingly, the scope of § 1001.2(b) is independent of how CFPA section 1002(15)(A)(xi)(II) is construed.

[124] 12 U.S.C. 5531, 5536.

[125] The CFPB notes that the scope of a "covered consumer financial product or service," as defined under § 1033.111(b) for purposes of part 1033, is not dependent on adopting § 1001.2(b). The products and services listed in § 1033.111(b) are already covered by existing statutory provisions such as CFPA sections 1002(15)(A)(i), (iv), (v), and (vii).

Statutory factors

Consistent with the proposal, the CFPB has determined that § 1001.2(b) meets the two factors set forth in CFPA section 1002(15)(A)(xi)(II). First, these activities are permissible for financial holding companies under the Federal Reserve Board's Regulation Y and for national banks under OCC regulations.[126] Both financial holding companies and national banks are permitted to engage, among other things, in data processing, data storage, and data transmission services by any technological means, so long as the data to be processed are financial, banking, or economic.[127]

No commenter disputed that the defined activities satisfy the first CFPA factor of being permissible for financial holding companies or banks. A research institute commenter did express concern that the definition could encompass activities that, in the commenter's view, are not financial. This commenter advocated that the CFPB borrow a test for financial activities from certain FTC regulations implementing the GLBA. However, this commenter did not argue that the financial data processing products or services covered by § 1001.2(b) are not permissible for financial holding companies or banks, which is the standard selected by Congress in the context of the CFPA. The commenter did not explain why the CFPB should use a test from a different regulatory framework instead of the CFPA standard, and accordingly the CFPB is relying on the CFPA standard.

With respect to the second CFPA factor, the processing of personal financial information has, or is likely to have, a material impact on consumers. As already discussed in the proposal

[126] 12 CFR 225.28(b)(14), 7.5006(a); *see also* 68 FR 68493, 68495-96 (Dec. 9, 2003) (explaining that 12 CFR 225.28(b)(14) permits bank holding companies to engage in a "wide range" of data processing activities, including bill pay services, financial data processing for marketing purposes, and delivering financial products or services over the internet, among other activities).

[127] *Id.*

and above in part I, use of personal financial data has become an even more important part of consumer finance than it was at the time that the CFPA was enacted in 2010. The processing of personal financial data, including storing, aggregating, and transmitting such data, has the potential to provide benefits to consumers but also expose them to a number of substantial risks. Financial data processing activities that are provided to consumers, assuming they are not already included within the definition of a financial product or service under CFPA section 1002(15)(A)(vii), raise the same type of consumer protection concerns as activities that do fall within this definition.

No commenter disputed the material impact of the activities covered by § 1001.2(b) on consumers. A bank expressed support for § 1001.2(b) as regulating nonbanks in a like manner as banks. A bank trade association argued that the provision should do more to cover data aggregators. However, the CFPB notes that § 1001.2(b) includes aggregating financial or banking data as an example of a financial data processing product or service.

Exclusions

Section 1001.2(b) states that it does not apply where the financial data processing is offered or provided by a person who, by operation of CFPA section 1002(15)(A)(vii)(I) or (II), is not a covered person. As background, CFPA section 1002(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 prescribed processing activities. CFPA section 1002(15)(A)(vii)(I) excludes from coverage 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. The CFPB is paralleling these exclusions in § 1001.2(b).

A research institute commenter argued that § 1001.2(b) should be amended to reflect CFPA section 1002(15)(C)(ii), which excludes "electronic conduit services" (as further defined in CFPA section 1002(11)) from the statutory definition of "financial product or service." However, it is unnecessary to specifically amend § 1001.2(b) along these lines, because, like other categories of financial product or service, § 1001.2(b) remains subject to the exclusion for electronic conduit services in CFPA section 1002(15)(C)(ii).[128] A trade association generally supported clarifying that financial data processing is a financial product or service under the CFPA. But it argued that "transmitting" financial data should be excluded from § 1001.2(b), because the trade association viewed it as distinct from financial data processing. However, financial data transmission is expressly covered by the applicable longstanding provisions of Regulation Y and OCC regulations, and it is within the scope of the CFPB's statutory authority if it is not an electronic conduit service as defined in CFPA section 1002(11).

Another trade association supported covering certain "retail" financial data services that are "consumer facing," but it advocated excluding what it described as "non-retail" services. The trade association argued that covering "non-retail" entities would reduce competition by limiting those entities' ability to efficiently use data. However, the CFPB cannot discern from the comment why the commenter believes this to be the case. The CFPB notes that Congress has

[128] *See* 12 CFR 1001.2 (introductory language stating that definitions apply except "as otherwise provided in [the CFPA]"). This commenter also argued that § 1001.2(b) should be amended to exclude certain persons who are excluded from the definition of "service provider" under CFPA section 1002(26)(a)(ii). That exclusion from the definition of "service provider" has similarities to the exclusion of electronic conduit services from the definition of "financial product or service." However, the commenter did not explain why the exclusion from the distinct statutory definition of "service provider" should be imported into the definition of "financial product or service," and the CFPB is not aware of a reason to do so. If the "service provider" exclusion applies to an entity, it would not be a service provider under the terms of the statute.

already established a boundary for a "consumer financial product or service" based on whether the product or service is "offered or provided for use by consumers primarily for personal, family, or household purposes" under CFPA section 1002(5)(A). Within that boundary, assuming a given financial data processing product or service would not have already been covered by CFPA section 1002(15)(A)(vii), the principal consequence of § 1001.2(b) is to protect consumers from unfair, deceptive, or abusive acts or practices under the CFPA. The CFPB does not agree that Congress's prohibition on subjecting consumers to unfair, deceptive, or abusive acts or practices interferes with fair competition.[129]

Finally, a consumer advocate commenter requested that the CFPB clarify that when an entity is covered by the CFPA through § 1001.2(b), that does not imply the entity is not covered by the Fair Credit Reporting Act. However, CFPA coverage does not foreclose an entity from being covered by other laws the CFPB administers, so the CFPB does not see a need to amend § 1001.2(b) to address the stated concern.

V. Effective and Compliance Dates

The effective date of the final rule is 60 days after the rule is published in the *Federal Register*. The CFPB proposed this effective date and did not receive any comments. As set forth in 12 CFR 1033.121, data providers must comply with the requirements in subparts B and C beginning April 1, 2026; April 1, 2027; April 1, 2028; April 1, 2029; or April 1, 2030, depending on the criteria set forth in § 1033.121(c). See part IV.A.5 for a discussion of the comments received with respect to compliance dates. In the case of the amendment to part 1001, the proposal explained that the activities covered by the amendment are already within the scope of

[129] *E.g.*, CFPA section 1031(c)(1)(B) (citing countervailing benefits to consumers and to competition as a factor when identifying unfair acts or practices).

the CFPA's definition of financial product or service, and it stated that no compliance date is necessary.[130] The CFPB received no comments on the implementation period for the amendment to part 1001, and accordingly it is finalizing the 60-day effective date as proposed.

VI. CFPA Section 1022(b) Analysis

A. Statement of Need

In section 1033 of the CFPA, Congress authorized and directed the CFPB to adopt regulations governing consumers' data access rights. The CFPB is issuing this final rule to implement CFPA section 1033 with respect to certain covered persons under the CFPA. The CFPB is also relying on other CFPA authorities for specific aspects of the rule.

Because the primary purpose of this rule is to implement section 1033 of the CFPA, the role of this CFPA section 1022(b) analysis is to evaluate the benefits, costs, and impacts of the specific policies within the rule and potential alternatives to those policies. This *Statement of Need* summarizes the CFPB's understanding of the gaps between Congress's intended outcome for consumers' financial data access rights and current practices, and describes the overall goals of the rule in closing those gaps. The remainder of the CFPA section 1022(b) analysis discusses the benefits, costs, and impacts of the specific provisions, and potential alternatives.

CFPA section 1033 requires data providers to make financial data available in electronic form upon request to consumers and third parties authorized to act on their behalf. Today, consumer financial data may be accessed by third parties through methods that raise data security and privacy risks, and consumers may have little to no knowledge of or control over how the data are used by third parties that have access to it. In addition, the market has been slow to

[130] Even assuming the activities covered by the amendment to part 1001 were not already within the scope of the CFPA's definition of financial product or service, the CFPB notes that it has no reason to believe a 60-day implementation period would be insufficient.

implement secure and efficient methods for sharing data with third parties, and data providers may not be motivated to provide in a timely and readily usable manner all the data fields that consumers may want to access. The result is that access to consumer financial data can be unreliable, or that financial data held by some providers may be unavailable to some consumers or their authorized third parties.

When data are made available, there is a general lack of consistency across data providers in the terms and conditions for access and the technical specifications used. This creates inefficiencies for market participants, and often entails substantial levels of cost.

This rule aims to (1) expand consumers' access to their financial data across a wide range of financial institutions, (2) ensure privacy and data security for consumers by limiting the collection, use, and retention of data that are not needed to provide the consumer's requested service, and (3) push for greater efficiency and reliability of data access across the industry to reduce industry costs, facilitate competition, and support the development of new products and services beneficial to consumers.

B. Data and Evidence

The CFPB's analysis of costs, benefits, and impacts is informed by data from a range of sources. These include data collected in the Provider Collection and Aggregator Collection,[131] as well as data obtained from other regulatory agencies[132] and publicly available sources.[133]

In 2016, the CFPB released and received comments on an RFI on consumer rights to access financial data. In 2020, the CFPB held a symposium titled "Consumer Access to Financial Records" and released a summary of the proceedings. Later in 2020, the CFPB released and received comments on an ANPR. In 2023, the CFPB convened a SBREFA Panel to gather input from small businesses and the Panel issued the SBREFA Panel Report.[134] The CFPB also solicited and received comments from other industry participants on the SBREFA Outline.[135] Later in 2023, the CFPB issued its proposed rule, and received comments from the public in response.[136] In addition to these sources of information, these impact analyses are informed by consultations with other regulatory agencies, industry, consumer advocates, and researchers. Part II.A further describes the CFPB's outreach.

---

[131] For information about the data collected in the Provider Collection and Aggregator Collection, respectively, *see* Consumer Fin. Prot. Bureau, *Generic Order for Data Providers*, https://files.consumerfinance.gov/f/documents/cfpb_generic-1022-order-data-provider_2023-01.pdf; and Consumer Fin. Prot. Bureau, *Generic Order for Data Aggregators*, https://files.consumerfinance.gov/f/documents/cfpb_generic-1022-order-data-aggregator_2023-01.pdf (both last visited Oct. 16, 2024). Because data providers and data aggregators vary substantially in size and business practices, the data from these collections are likely not representative of the market as a whole. The data are informative about the practices of some large data providers and a selection of data aggregators and third parties.

[132] In particular, these include entity-level FFIEC and NCUA data on characteristics of depository institutions.

[133] The analysis is informed by academic research papers, reports on research by industry and trade groups, practitioner studies, and comment letters received by the CFPB. Where used, these specific sources are cited in this analysis.

[134] Consumer Fin. Prot. Bureau, *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), https://files.consumerfinance.gov/f/documents/cfpb_1033-data-rights-rule-sbrefa-panel-report_2023-03.pdf.

[135] Consumer Fin. Prot. Bureau, *CFPB Kicks Off Personal Financial Data Rights Rulemaking* (Oct. 27, 2022), https://www.consumerfinance.gov/about-us/newsroom/cfpb-kicks-off-personal-financial-data-rights-rulemaking/.

[136] *See* 88 FR 74796 (Oct. 31, 2023).

For the types of financial data and access generally covered by this rule, the information obtained through the Provider Collection and Aggregator Collection allow the CFPB to estimate: the number of data providers consumer-authorized data are accessed from; the number of third parties accessing or using consumer-authorized data; the number of consumers granting third parties permission to access data on their behalf; the total number of permissioned access attempts; and information about the technologies used and the purposes of the permissioned data access. The Provider Collection and Aggregator Collection also allow the CFPB to estimate the operational costs of providing direct and third party data access, and the costs of establishing data access agreements. To maintain the confidentiality of the respondents to these data collections, the CFPB provides approximate or bounded estimates derived from these data, rather than precise totals or figures specific to any one respondent.[137]

In the proposal, the CFPB requested additional information or data that could refine these estimates. Where commenters provided such information, it is discussed in the relevant part and incorporated into the analysis and estimates.

For data on the number and characteristics of covered depository institutions, the CFPB relies on data from FFIEC and NCUA Call Reports.[138] These sources provide quarterly information on the number of institutions, dollar amount of institution-level assets, number of deposit accounts, dollar volume of credit card lending, and other characteristics. Notably, these data provide information on the number of deposit accounts insured by the FDIC or NCUA, which are imperfect, but nonetheless the best available proxy for the number of covered financial

[137] The CFPB treats the information received in the Provider Collection and the Aggregator Collection in accordance with its confidentiality regulations at 12 CFR 1070.40 *et seq.*

[138] *See* Fed. Fin. Insts. Examination Council, *Central Data Repository's Public Data Distribution*, https://cdr.ffiec.gov/ (last visited Oct. 16, 2024); and Nat'l Credit Union Admin., *Credit Union and Corporate Call Report Data*, https://ncua.gov/analysis/credit-union-corporate-call-report-data (last updated Sept. 5, 2024).

accounts held by depositories. While this measure includes covered depository accounts, it also includes business accounts and other accounts that are not covered by the rule. It also does not include certain covered financial accounts, such as credit card accounts and non-bank products. The FFIEC data also provide information on the websites and digital banking capabilities for banks. The CFPB supplemented this information with comparable information in NCUA Profile (Form 4501A) data for credit unions.[139]

To estimate costs to small entities of the provisions, the CFPB relies on information gathered from the SBREFA process and from comments on the proposal. This includes written feedback on the SBREFA Outline submitted by small entity representatives, the discussions at the SBREFA Panel summarized in the SBREFA Panel Report, and comments on the proposal.

C. Coverage of the Rule

Part VII.B.4 provides a discussion of the number and types of entities affected by the rule. Relative to the proposal, the most substantial change in coverage is that depositories with assets below specified size standards defined by the SBA are not covered as data providers under the rule.

D. Baseline for Consideration of Costs and Benefits

In evaluating the rule's benefits, costs, and impacts, the CFPB considers the impacts against a baseline in which the CFPB takes no regulatory action. This baseline includes existing regulations, State laws, and the current state of the market. In addition, because the market is still developing rapidly, the analysis assumes that the market trends toward greater data access and increased adoption of developer interfaces would continue under the baseline, but assumes no

[139] *See* Nat'l Credit Union Admin., *CUOnline*, https://ncua.gov/regulation-supervision/regulatory-reporting/cuonline (last updated Sept. 18, 2024).

change in the State laws and regulations currently in effect that are related to consumers' data access rights for either direct access or access through third parties.

A large and growing number of consumers currently access their financial data through consumer-authorized third parties. This access is provided by a range of technologies, including credential-free APIs, APIs that require third parties to retain consumer credentials (credential-based APIs), and credential-based access through consumer-facing digital banking interfaces such as online banking websites or mobile applications (screen scraping). As discussed in part I.B, with respect to the state of the open banking system, the CFPB estimates that more than 100 million consumers have used consumer-authorized data access, authorizing thousands of third parties to access their financial data at thousands of data providers, often through intermediaries such as data aggregators.[140]

In total, the CFPB estimates that there were between 50 billion and 100 billion total consumer-authorized access attempts in 2022.[141] Usage has grown substantially in recent years, as the annual number of consumer-authorized access attempts approximately doubled from 2019 to 2022, and usage has continued to grow since 2022.[142]

[140] Unless described otherwise, the estimates in this part VI.D are derived from the total numbers of consumers, connections, and access attempts reported by data providers in the Provider Collection and third parties in the Aggregator Collection. These estimates are necessarily approximate, as the CFPB aims to protect the confidentiality of the respondents, account for the substantial share of consumer-authorized data sharing that is not captured by the respondents, and account for the likely potential overlap in counts for consumers, connections, and access attempts that involve respondents to both the Provider Collection and the Aggregator Collection.

[141] An access attempt is defined here as an individual instance in which a single consumer-authorized third party requests or attempts to pull data about a single consumer's accounts from a single data provider's systems. Not all attempts will lead to a successful data transfer, but the number of access attempts is used as an indicator for the overall size and growth of the open banking system.

[142] *See* Fin. Data Exch., *Financial Data Exchange (FDX) Reports 76 Million Consumer Accounts Use FDX API* (Mar. 13, 2024), https://www.financialdataexchange.org/FDX/News/Press-Releases/Financial_Data_Exchange__FDX__Reports_76_Million_Consumers_Use_FDX_API.aspx.

This third party financial data access enables numerous use cases for consumers. In 2022, data available to the CFPB show that there were more than two billion access attempts to facilitate payment services, more than one billion access attempts for the purpose of identity verification (typically for opening new accounts), tens of billions of access attempts for account monitoring and personal financial management use cases, and over one billion access attempts facilitating other use cases, including fraud risk assessments, loan underwriting, and asset and income verification.

While the share of consumer-authorized data accessed through dedicated credential-free APIs has grown sharply, many access attempts still rely on either credential-based APIs or screen scraping. As a share of all access attempts made by firms in the Aggregator Collection, the use of credential-free APIs grew from less than 1 percent in 2019 and 2020 to 9 percent in 2021 and 24 percent in 2022. At the same time, the share of access attempts using screen scraping declined from 80 percent in 2019 to 50 percent in 2022. Credential-based APIs saw a slight increase from 20 percent in 2019 to 27 percent in 2022.

The recent growth in traffic through credential-free APIs reflects the adoption of this technology by some of the largest data providers, covering tens of millions of covered accounts. All depository data providers with more than $500 billion in assets have established, or in the near future will establish, a credential-free API. However, despite recent growth, the total share of data providers offering credential-free access methods remains limited. At the end of 2022, an estimated 5 to 10 percent of all data providers offered credential-free APIs, up from less than 1 percent in 2021. The adoption of credential-free APIs by core banking service providers and

other vendors that serve hundreds of smaller depository institutions contributed to this growth.[143] While adoption is relatively high for the largest depository data providers, the CFPB estimates that only 10 to 20 percent of depositories with more than $10 billion in assets had credential-free APIs at the end of 2022.

The future evolution of the marketplace enabled by the exchange of consumer financial data is uncertain. Based on the data and market trends available, the CFPB makes the following assumptions for the baseline in this impact analysis. The analysis assumes that most of the largest data providers have adopted or likely would in the near future adopt credential-free APIs, which would meet many—but likely not all—requirements contained in the rule. Awareness of CFPA section 1033 may have contributed to this, though adoption is also influenced by data providers' desire to shift third party access away from screen scraping and towards more secure and efficient technologies, as well as the demand for third party access from data providers' customers. The analysis also assumes that some share of smaller institutions would adopt credential-free APIs, depending on their technology and business models, over a longer-term horizon. Based on past trends, larger institutions would be more likely to adopt such interfaces sooner. However, adoption may be easier for (1) depositories whose systems are already well integrated in-house or with large core banking or online banking service providers and (2) nondepositories and newer depositories that do not have complex legacy systems, irrespective of the sizes of these types of institutions. In addition, in the current market some data providers block screen scraping access under certain circumstances, including for third party risk management, and the CFPB expects this would continue under the baseline.

[143] For example, *see* Press Release, Jack Henry & Assocs., Inc., *Jack Henry Partners with Open Banking Providers to Enhance Digital Platform* (Oct. 12, 2021), https://ir.jackhenry.com/news-releases/news-release-details/jack-henry-partners-open-banking-providers-enhance-digital.

The CFPB understands that all or most third parties seeking to access consumer-authorized information and data providers are subject to the GLBA, specifically either the FTC's Safeguards Rule or the prudential regulators' Safeguards Guidelines. Additionally, third parties that operate in one of the at least 11 States with consumer data privacy legislation may be subject to other data security requirements and data usage restrictions. These State laws have all been passed since 2018. Depository data providers also have third party risk management obligations required by their prudential regulators, which will impose data security requirements on third parties seeking to access consumer-authorized data. As a result, at baseline, the CFPB expects that many third parties are already subject to statutory and regulatory data privacy and security obligations, and third parties have adopted or would adopt some basic standards related to risk management, data security, and data use. These standards likely have some degree of overlap with the requirements in the rule, though individual company systems or policies will depend on the size, location, practices, and other circumstances of each third party.

Several commenters expressed concerns about how the rule may interact with other existing or future regulations. A credit union and a bank trade association asserted that the CFPB estimated costs in isolation of other regulations, including those from prudential regulators. Two data aggregators commented that data providers will invoke third party risk management obligations to deny access in anticompetitive ways. SBA Advocacy and a trade association commented that the CFPB should consider current or future State laws that may have similar requirements.

The CFPB has considered existing regulations and laws that interact with the rule, as these are part of the baseline for this impact analysis. Any costs of complying with existing regulations and laws are thus included in the baseline, and this analysis is of changes in costs

relative to that baseline. The impact analysis does not consider the effects of potential future laws or regulations that may interact with the rule, as this would be overly speculative given the uncertainty around them.

The impact analysis generally includes the major elements of costs to firms of complying with the rule. It also includes a discussion of how some of these costs likely would have been borne under the baseline as data providers either would have adopted or already have adopted systems or policies similar to those required by the rule. For example, where data providers have adopted some form of credential-free third party access under the baseline, the analysis discusses how the rule will impact the terms, costs, and features of such functionality.

Finally, in the context of direct access, the proposal assumed for its baseline that all covered data providers offer consumers some digital banking interface and that these interfaces typically provide all or nearly all data fields required to be made available by the proposal. The CFPB maintains this assumption in the final rule, as the CFPB understands that all or nearly all data providers within the rule's revised coverage offer consumer interfaces. Comments related to the costs of building and maintaining such interfaces for direct access from data providers are discussed in part VI.E.1. The analysis considers how the rule will impact the costs and features of data providers' consumer interfaces.

E. Potential Benefits and Costs to Consumers and Covered Persons

The analysis below describes the potential benefits and costs to consumers and covered persons in the following order: costs to data providers, costs to third parties, costs to consumers, benefits to data providers, benefits to third parties, benefits to consumers, and alternatives considered.

A service provider for credit unions asserted that the CFPB should engage in a more thorough cost-benefit analysis and that the CFPB did not gather enough input or data from core providers. Trade associations for credit unions and businesses claimed that the proposal's analysis was incomplete, some elements had not been justified, and that the CFPB had failed to engage in a thorough and accurate analysis. The CFPB considered all of the data and evidence described in part VI.B, including all comments on the proposal, in analyzing the potential benefits and costs of the rule. The CFPB does not have the data to precisely determine every potential benefit and cost of the rule, but requested comment on the proposal for additional data or evidence that could refine the estimates of benefits and costs. The CFPB has reasonably evaluated all such evidence provided, and updated its estimates where appropriate.

Where commenters stated that the CFPB had failed to justify or address the benefits and costs of particular provisions of the proposal, those comments are discussed in this part.

1. Costs to covered persons

Costs to data providers

As a result of the rule, covered data providers may face increased costs related to maintaining consumer interfaces and establishing and maintaining developer interfaces, including modifying their existing systems to comply with the rule. The CFPB expects the largest costs to data providers to come from establishing and maintaining data access for authorized third parties in accordance with rule requirements. Covered data providers will also incur costs related to developing and implementing policies and procedures governing those systems. The rule may have additional costs to covered data providers related to changes in the frequency, scope, or method of consumer-authorized data access relative to the baseline. These changes may have secondary effects on the profitability of certain business models or practices,

including by facilitating competition and enabling new products and services. The estimation of data providers' costs described in this section broadly uses the same methodology that the CFPB used in the proposal unless otherwise noted. The primary differences are adjustments to the costs of developing policies and procedures that are informed by comments.

Maintaining direct consumer access

The rule requires covered data providers to make covered data available through consumer interfaces and to allow consumers to export certain information in machine-readable formats. As discussed in part IV.A.2, small depository institutions are not required to comply with the final rule's requirements applicable to data providers. During the SBREFA Panel meetings, the CFPB received feedback that certain categories of information under consideration in the SBREFA Outline are not typically made available directly to consumers, and thus would be costly to provide.[144] Based on this feedback, the rule covers a more limited set of information, which the CFPB understands is currently provided through existing consumer interfaces by all or nearly all data providers. Therefore, for most data providers, the CFPB expects limited additional costs due to the rule's direct consumer access requirements. For those data providers that do not provide all required information under the baseline, the CFPB expects that such information could be added at relatively low cost because the required information is generally already necessary for compliance with other regulatory requirements, like providing account opening disclosures. The CFPB does not have sufficient data to quantify the levels of these costs.

In the proposed rule, the CFPB sought comment or information on the costs of adding data fields to the consumer interfaces but did not receive any. A trade association for nondepository service providers commented that the costs would be high to create a consumer

[144] SBREFA Panel Report at 24.

interface for nondepository institutions that do not have one already but did not provide additional information on the magnitude of the cost. A few other commenters asserted that the rule will raise costs and barriers to entry for retailers to develop and use pass-through digital wallets, if those products are covered as data providers. The CFPB expects that few nondepository data providers that are covered by the rule do not already have a consumer interface. The CFPB acknowledges that those few nondepository data providers could incur additional costs associated with creating a consumer interface but does not have sufficient data to determine the magnitude of these costs.

Maintaining third party access

The rule requires data providers to maintain data access through a compliant developer interface. Although many data providers already maintain similar functionality, others would need to establish new interfaces, likely integrated with existing infrastructure that supports their consumer interfaces. However, unlike the proposal, the rule does not require small depositories to maintain data access for authorized third parties, meaning many fewer institutions than estimated in the proposal will need to provide data access functionality under the rule. The CFPB expects that the costs of modifying existing infrastructure to ensure compliance with the rule will depend on the scope and nature of the necessary modifications but would generally be lower than the cost of establishing a new interface.[145]

In general, data providers must either contract with a vendor for the required functionality or develop and maintain it in-house. The analysis below estimates compliance costs under these two approaches. Some data providers may comply with the rule through a combination of

[145] For example, some data providers with existing interfaces may need to provide additional data fields, change the way their data are formatted, or make additional investments to ensure their interfaces meet the performance specifications required by the proposed rule.

contracted services and in-house development. Because data providers will generally choose the lowest-cost approach, their costs will generally be at or below the lower of the costs of the two feasible alternatives analyzed here.

The CFPB understands that data providers' costs depend on many factors and the extent to which they vary is impossible to fully capture. To produce cost estimates that are practical, meaningful, and transparent, where feasible, the CFPB estimates initial upfront costs and annual costs that generally scale with the size of the data provider for each of the contracted services and in-house approaches. All else equal, a data provider's annual cost per account or per customer is likely to decrease with a greater number of accounts or customers due to economies of scale. During the SBREFA process and in the Provider Collection, some data providers provided cost estimates per account while others estimated costs per customer. Therefore, the analysis below discusses estimates of the annual cost per account or per customer of operating a compliant developer interface that are likely to be appropriate for data providers of different sizes.

Under the contracted services approach, data providers would primarily contract with a vendor for the necessary functionality. At baseline, many covered data providers contract with core banking providers or other vendors for transaction processing, online banking systems, or other key banking functions. Some core banking providers currently offer services to enable developer interfaces for data providers. The CFPB understands that some large core banking providers provide their clients with a basic developer interface at no additional cost.[146] Based on comments received during the SBREFA process and market research, the CFPB understands that

[146] For example, *see* Jack Henry & Assocs., Inc., *Secure Data Connection: take back control of account connection*, https://banno.com/data-aggregators/ (last visited Oct. 16, 2024).

other core banking providers charge flat monthly fees or per-account fees.[147] The CFPB understands that these fees vary but generally estimates that fees can be up to $24 per account per year.[148]

Data providers taking this approach will generally have minimal upfront costs to enable the required third party access. However, some data providers use service providers that do not currently offer this kind of functionality. Although other options exist and the CFPB expects service providers would face strong competitive pressure to offer compliant developer interfaces to their clients, the lowest cost option for some data providers may involve changing their core banking provider. The fixed costs of changing core banking providers can be high. Several small entity representatives stated that the upfront costs at a new core banking provider can range from $50,000 to $350,000 depending on the scale and complexity of the system, with up to $200,000 in additional decommissioning costs to retrieve information from the old core banking provider. While small depository institutions are not required to comply with this final rule, many medium-sized depository institutions also rely on core providers. The CFPB expects that the medium-sized depository institutions may pay closer to $350,000 due to scale and complexity if they need to switch to a new core provider that offers a compliant developer interface. Based on its market research, the CFPB understands that core banking providers that offer a developer interface have a combined market share exceeding 67 percent.[149] Therefore, at most, 33 percent of depository data providers would need to change core banking providers to obtain a compliant interface that is bundled with their other core banking services. However, the CFPB expects that

[147] SBREFA Panel Report at 37.

[148] *Id.* at 38.

[149] *See* Press Release, Fiserv, *Finicity and Fiserv Offer More Consumer Choice Through Secure Data Access* (Mar. 30, 2022), https://newsroom.fiserv.com/news-releases/news-release-details/finicity-and-fiserv-offer-more-consumer-choice-through-secure.

the true share of covered depository data providers that pay these costs will be much lower than 33 percent. Data aggregators and other software vendors offer developer interfaces and the CFPB expects that some data providers will obtain the necessary functionality through these channels and will not need to change their core banking provider. Furthermore, core banking providers will face strong competitive pressure to offer compliant developer interfaces to retain their clients and potentially capture additional market share. The CFPB expects that these forces are likely to cause the cost of obtaining compliant interfaces to decline over time, which may reduce compliance costs most substantially for smaller covered depository data providers, given that they have the latest compliance date.

The CFPB requested information related to the developer interfaces offered by core banking providers and other vendors and how such interfaces are priced. The CFPB received several comments on the costs associated with the contracted services approach. Several banks and credit unions confirmed that depository institutions will depend on core banking providers to obtain the necessary functionality. A credit union trade association and two banks asserted that these core providers are likely to charge additional fees to provide these services. A credit union suggested that an API could cost between $50,000 and $125,000 from a core provider. A bank commented that they may also incur associated personnel costs but did not provide additional information on the magnitude of the costs. A credit union asserted that, if a depository institution is required to switch to a new core provider to obtain a developer interface, the waiting period to switch is about two years and thus the depository would not be able to comply by the mandatory compliance dates. Another credit union, however, commented that core providers would be implementing solutions for all depositories and, thus, expects costs per data provider to be manageable. Similarly, a consumer advocate commented that they expect industry utilities and

cloud providers could keep costs manageable. Finally, a service provider for credit unions commented that the CFPB did not gather enough input from core providers in estimating these costs.

The CFPB acknowledges that core providers may charge data providers to provide the required functionality. The CFPB developed its cost estimates in the proposal based in part on feedback from small entity representatives received through the SBREFA process, and considers the information provided by commenters about core providers to be broadly consistent with the CFPB's estimated costs. Furthermore, the commenters most concerned about the costs of contracting with core providers to enable the required third party access were small depository institutions that will not be required to comply with the data provider requirements of this final rule.

Under the in-house approach, data providers would primarily employ software developers or similar staff to build and operate the necessary functionality. The estimates below are based on a fully in-house approach for developing of a compliant developer interface. Some data providers may instead contract with software providers for the initial development of their in-house developer interface. The CFPB anticipates that data providers would purchase their systems only if they could do so at a lower cost than the estimate of building a compliant interface provided here.

The CFPB expects that most data providers that have already developed and have been maintaining consumer interfaces in-house would also develop and maintain the required developer functionality in-house.[150] In the proposal, the CFPB estimated that for smaller data

[150] As discussed below, large depository data providers have generally indicated that the resources required to maintain the required third party access in-house are a small fraction of the resources required to maintain consumer interfaces in-house. Therefore, the CFPB expects that data providers that have already invested in the capacity to

providers, developing a compliant interface for third party access would likely require between 2,600 and 5,200 hours of work by software developers or similar staff, equivalent to five full-time employees over a period of three to six months, resulting in an estimated total upfront staffing cost of $237,000 to $475,000, which the CFPB has updated to $247,000 to $494,000 for the final rule based on more recent labor cost data.[151] However, these estimates strongly depend on the needs and capabilities of specific entities. For example, based on feedback from nondepository small entity representatives, the CFPB estimated in the proposal that nondepository data providers may require only 480 hours of work by software developers at a total cost of $44,000, which the CFPB has updated to $46,000 based on more recent labor cost data.[152]

In addition to these upfront costs, the CFPB estimated that data providers taking the in-house approach would incur ongoing costs. In the proposal, the CFPB estimated that small data providers (both depository and nondepository) would incur ongoing annual technology costs of $20,000 as well as ongoing staffing costs of $45,000 to $91,000, which the CFPB has updated to $48,000 to $95,000 based on more recent labor cost data.[153] Under the final rule, small

operate a consumer interface in-house will take a similar approach to providing the required third party access. However, it is likely that some data providers will find it less costly to contract with service providers. As the industry develops, it is possible that it will become more common for data providers to enable third party access through service providers.

[151] This estimate was derived from BLS data showing a mean hourly wage for software developers of $66.40. BLS data also show that wages account for 70 percent of total compensation for private industry workers, leading to a $94.86 estimate for total hourly compensation, which was multiplied by the expected total number of hours of work required.

[152] Costs for depository and nondepository data providers are likely to differ for several reasons, including that depository data providers are generally more likely to have multiple legacy information technology systems that are more technically difficult to integrate with a developer interface.

[153] The CFPB estimates that small data providers choosing the in-house approach would require 500 to 1,000 hours per year of staff time by software developers. BLS data from May 2023 shows a mean hourly wage for software developers of $66.40. BLS data also show that wages account for 70 percent of total compensation for private industry workers, leading to a $94.86 estimate for total hourly compensation, which was multiplied by the expected total number of hours of work required.

depositories will not have costs for complying with the data provider requirements of the rule. For medium-sized data providers with more accounts, the CFPB estimated ongoing costs of $5 per account per year to maintain the required functionality in-house, based on evidence from the Provider Collection described below.

The Provider Collection contains information on costs for a sample of large depository data providers. This complements the information on costs for small data providers gathered through the SBREFA process. For context, data provider small entity representatives generally may have up to a few tens of thousands of accounts, while data providers in the Provider Collection have millions of accounts.

In the Provider Collection, several data providers stated that it was difficult to disaggregate the costs of developer interfaces from their consumer interfaces and other information technology systems. These data providers also generally provided estimates of ongoing annual costs or total costs since the deployment of their developer interfaces, rather than upfront costs to build an interface. Reported estimates of the cost of establishing and maintaining a developer interface varied widely, from $2 million to $47 million per year, with a median of $21 million per year. Of the data providers providing disaggregated estimates, the median cost of developer interfaces as a share of the cost of their consumer interfaces was 2.3 percent. An additional data provider did not provide a disaggregated estimate but reported their developer interface constituted a "small portion of the total consumer-portal costs."

These data providers are larger and more complex than most data providers. Therefore, the CFPB adopts the cost of a compliant developer interface per account as the relevant metric for estimating the costs for data providers generally. The reported cost of an in-house developer interface per customer or account ranges from $0.25 to $8 per year, with a median of $3.37 per

year, substantially lower than the $24 per year reported by small entity representatives as the potential cost for the contracted services approach. Within the sample, the per account cost generally declined as the number of accounts increased.[154] Based on this evidence, the CFPB estimates that annual costs per account to maintain an in-house developer interface are likely to be approximately $3 for large depository data providers and $5 for medium-sized depository data providers. Although the Provider Collection sample is relatively limited, the pattern of per-account costs declining with the number of accounts suggests that—relative to the alternative of contracting for a developer interface—data providers developing and maintaining interfaces in-house likely have larger upfront fixed costs but smaller ongoing per account costs. These estimated costs are generally for depository institutions rather than nondepositories. Given feedback from small entity representatives of nondepository institutions that would qualify as data providers under the rule, the CFPB expects that nondepository data providers would generally have less need to integrate across multiple systems and would be less likely to have legacy software that is difficult to update, resulting in lower costs on average.

The estimates above relate to the costs of developing and maintaining a developer interface for data providers without such existing interfaces. Covered data providers with existing developer interfaces that are not fully compliant with the proposed rule would incur smaller costs to modify their interfaces and existing third party access agreements to align with the requirements of the rule. The cost for such covered data providers would depend on the extent to which their developer interfaces do not comply with the requirements of the proposed rule. Without granular data on the nature of partially compliant interfaces, the CFPB cannot

[154] For the data providers in the Provider Collection that provided both cost estimates and numbers of accounts, there was a negative correlation coefficient of approximately -0.6 between per account costs and number of accounts.

provide a precise estimate of the cost of bringing such systems into compliance with the rule. However, that cost will generally be a fraction of the cost of developing and maintaining a new interface.

In the proposal, the CFPB sought comment or additional data on the costs associated with modifying an existing developer interface or establishing a new compliant developer interface, including how those costs compare to contracting with a service provider. Many community banks, credit unions, and related trade associations commented that they expect the costs of the required functionality to be much higher for small depository institutions than those estimated by the CFPB. These commenters did not provide additional data or information that would allow the CFPB to precisely update the costs for small depositories estimated in the proposal. The CFPB acknowledges that small depository institutions may have faced additional challenges to implement the rule at this time and is not requiring small depository institutions to comply with the final rule's requirements on data providers. Accordingly, the CFPB has not updated the estimates for small depository institution data providers.

Several banks, credit unions, and their respective trade associations asserted that the CFPB underestimated compliance costs for data providers, failed to consider all costs, and underestimated the technical challenges associated with the proposal. A bank and a credit union asserted that the incremental costs associated with the increased number of data requests will not be minimal on a per-account basis. A credit union and several credit union trade associations asserted that the CFPB's per-account cost estimates were not appropriate for smaller depository institutions because those estimates were primarily derived from information provided by large data providers. These commenters generally did not provide additional data or information that the CFPB could use to modify the cost estimates and instead requested additional study before

finalizing the rule. One bank requested that the CFPB estimate expected transaction volumes, customer service staffing, IT systems and security protocols, and how these may depend on the size of the data provider.

The CFPB acknowledges that some data providers may incur larger costs than those discussed in this section. The costs associated with implementing the rule will be data provider-specific and the estimated costs discussed here should be considered the average expected costs for a data provider. Had small depositories been required to comply with the final rule's requirements on data providers, the CFPB acknowledges that they may have faced higher or more uncertain costs than discussed here to comply with the final rule. The CFPB has considered the information from the comments, together with the Provider Collection and SBREFA panel, and has determined that the estimates discussed in this section are appropriate for the data providers that are covered by the rule.

Commenters representing bank trade associations stated that some data providers would incur significant costs to comply with the rule, even if they already have an existing interface for third party access. Several bank trade associations noted that banks have already spent hundreds of hours assessing compliance and designing potential solutions and modifications that may be needed to comply with the rule. One trade association asserted that the rule could cost as much as $100 million in the first year and an additional $15 million each year to update and maintain a compliant developer interface, although the trade association did not specify how they obtained these estimates. The CFPB acknowledges that data providers that already have a third party interface may incur costs to update and maintain that interface to comply with the rule and notes that $15 million in annual ongoing costs is consistent with the CFPB's estimates for large data providers with millions of accounts. However, given the information contained in the comment,

the CFPB considers the magnitude of the provided estimate of costs for the first year to be overstated, particularly given the rule's extended compliance timelines for large data providers relative to the proposal.

A bank commented that the CFPB failed to account for compliance costs of reviewing requests and monitoring consumer authorizations. In this analysis, these costs are accounted for in the ongoing costs associated with maintaining a developer interface, but the CFPB acknowledges that some data providers may incur higher levels of cost than others.

Two credit unions commented that the CFPB underestimated costs of the revocation mechanism. Data providers are permitted but not required to offer a developer interface that lets consumers revoke third party access. The CFPB does not include costs associated with an optional feature.

Many data providers and SBA Advocacy commented that the lack of clarity on what the proposal had referred to as a "qualified industry standard" would create confusion and increase compliance costs, particularly for smaller data providers, and requested additional guidelines for the consensus standards and standards setting body. As discussed in part II.C, the Industry Standard-Setting Rule finalized in June 2024 specifies the attributes standard-setting bodies must satisfy to receive CFPB recognition as a recognized standard setter capable of adopting consensus standards (referred to under the proposal as a qualified industry standard). Under the final rule, conformance with consensus standards serve as indicia of compliance for various provisions of the final rule. The CFPB has determined that the Industry Standard-Setting Final Rule and the references to consensus standards in this rule will mitigate the cost concerns of these commenters (assuming the consensus standards comply with the final rule), particularly given the extended compliance timelines in the final rule.

Developing and implementing policies and procedures

The rule includes disclosure and recordkeeping requirements for all covered data providers related to consumer-authorized data access. The rule requires data providers to calculate and disclose the response rate for third party data access on a monthly basis. The CFPB understands that a variety of performance metrics, including the response rate, may be calculated in the normal course of operating an API or other digital interface for diagnostic purposes. Therefore, the cost of this provision is included in the cost of developing and maintaining a compliant developer interface estimated above. Data providers may incur an additional upfront cost of developing and testing a system to regularly disclose required performance metrics on their website. The CFPB estimates that this process would take less than 80 hours of staff time at an estimated cost of $7,600 per data provider.[155] The CFPB expects that once the disclosure system is implemented it would be maintained at minimal incremental cost as part of the overall cost of operating data providers' websites.

The rule requires data providers to have policies and procedures such that the developer interface is reasonably designed to ensure that data are accurately transferred to third parties. The CFPB expects that data providers would comply with this requirement as part of establishing and maintaining a compliant developer interface. Therefore, the costs of ensuring that the developer interface is reasonably designed to transfer data accurately are included in the analysis above.

The rule also requires data providers to have policies and procedures reasonably designed to ensure that the reason for the decision to decline a third party's request to access its interface is communicated to the third party. The requirements to inform third parties when and why

[155] This estimate was derived from BLS data showing a mean hourly wage for software developers of $66.40. BLS data also show that wages account for 70 percent of total compensation for private industry workers, leading to a $94.86 estimate for total hourly compensation, which was multiplied by the expected total number of hours of work required.

access was not permitted would generally be satisfied as part of the onboarding process in cases of reasonable denials related to risk management or built into a data provider's developer interface, as automated responses to third party data access requests. Similarly, the requirements to retain records to demonstrate compliance with certain requirements of the proposal would generally be built into a data provider's developer interface. As a result, the CFPB considers the costs of complying with these requirements as part of the overall costs of the onboarding process or implementing a compliant developer interface, as described elsewhere. The CFPB has previously estimated that, to comply with a rule of similar complexity, a data provider will require several categories of one-time costs.[156] The CFPB has added several categories of one-time costs relative to the proposal in response to the comments discussed below. The CFPB has also adjusted the estimates to account for inflation. Each covered data provider is expected to incur the following costs: $9,000 to $25,000 for preparation and planning; $3,100 to $5,200 for developing policies and procedures; $3,700 to $8,900 for legal and compliance review; $3,900 to $5,600 for developing forms and disclosures; and $3,800 to $6,500 for training staff and vendors on the new policies and procedures.[157] The CFPB estimates a total one-time cost of developing and implementing policies and procedures as required by the proposed rule of $23,500 to $51,200 per data provider.

A nondepository entity trade association commented that the proposal's cost estimates for updating policies and procedures were too low. A bank requested that the CFPB determine the costs associated with developing disclosures and account agreement changes. The CFPB has adjusted the costs associated with developing policies, procedures, disclosures, and agreements

[156] 88 FR 35150, 35497 (May 31, 2023).

[157] *Id.* at 35150.

in the final rule. A bank commented that it was not practical to provide some information, such as terms and conditions, in a machine-readable format. As discussed in part IV.C.2., the rule does not apply the machine-readability requirements to terms and conditions and some other consumer information provided through the consumer interface. However, the CFPB has determined that it is necessary to make that information available in a machine-readable form through the developer interface.

Two trade associations for depositories asserted that the proposed record retention requirements for data providers would require providers to keep track of, and report on, all data collected about consumers, which would create large costs. The rule does not require that data providers keep records about all data collected about consumers. Instead, the rule requires that data providers retain records related to third party requests for access to its interface, requests for information, third party authorizations, revocation requests made through the data provider, and performance specifications, as discussed in part IV.C.7. Additionally, some bank commenters suggested a shorter retention period than three years for information related to data accessed through the developer interface, though at least one bank trade association commenter supported the three-year retention period. The CFPB has determined that the record retention requirements will provide the data necessary to facilitate effective supervision and enforcement of compliance with the rule.

Indirect costs

In addition to the direct costs described above, data providers are likely to incur indirect costs as a result of the rule. The CFPB expects costs related to onboarding additional third parties relative to baseline as well as changes in the frequency, scope, or method of consumer-authorized data access relative to the baseline. These changes may have secondary effects on the

profitability of certain business models or practices, including by facilitating competition and enabling new products and services.

Costs from onboarding additional third parties

The rule generally requires data providers to grant access to their developer interface, except for reasonable denials related to risk management or the absence of certain information about themselves. Although the rule does not require formal data access agreements, the CFPB expects the rule to lead to more third parties requesting and being granted access to data providers' developer interfaces relative to the baseline. The CFPB expects that this is likely to require data providers to enter into more onboarding arrangements with third parties. In the Aggregator Collection responses, which reflect costs applicable under the baseline, aggregators reported that negotiating a data access agreement with a data provider could take between 50 and 4,950 staff hours for business relationship managers, software developers, lawyers, compliance professionals, and senior management, depending on the complexity of the negotiation. The median estimated time was 385 staff hours per agreement. The CFPB expects that data providers currently spend roughly equivalent time and resources negotiating and signing data access agreements at baseline.

These costs are likely to decrease under the rule relative to the baseline because many features of interface onboarding arrangements are now regulated by the rule and not subject to negotiation, including requirements for interface reliability, fees, the scope of data accessible via the interface, authorization procedures, and the duration of access to consumers' covered data. One firm in the Aggregator Collection stated that in cases where data providers agree to use existing industry-defined standards there is essentially no need for negotiation. The CFPB expects that under the rule nearly all data providers will use standardized onboarding

arrangements and the costs of establishing data access will generally be limited to ensuring third party risk management standards are satisfied and performing any administrative tasks to provide third parties with access to the developer interface. In the proposal, the CFPB estimated that this process would require 80 staff hours on average, representing approximately $6,800. These costs may be further reduced if industry accreditations or consensus standards develop to streamline data providers' required efforts on third party risk management, or to the extent that prudential regulators provide further guidance applicable to sound risk management in the specific context of consumer-authorized data access. While some data providers and third parties may choose to use a customized arrangement that respects the terms of the rule, they will generally only do so when both parties perceive that the benefits exceed the costs. Because the choice to negotiate a costly but more customized arrangement is a business decision not required by the rule, the additional costs of doing so are voluntarily acceded to and are generally outside the scope of this analysis.[158]

The total cost of entering into onboarding arrangements will depend on the difference between the number of agreements that would be negotiated under the baseline and the number of onboarding arrangements that would be entered into under the rule. Because the consumer-authorized data access system is developing rapidly, it is not possible to precisely estimate the number of additional connections that would be established by the rule. However, in the near term, the CFPB anticipates that most data providers will continue to provide third parties access to consumer-authorized data through specialized intermediaries like data aggregators, as they would have under the baseline. As a result, the CFPB estimated in the proposal that, on average,

[158] To the extent that data providers choose to voluntarily enter into additional customized arrangements in response to the rule, the CFPB expects the benefits to data providers of such arrangements to exceed any additional upfront costs from establishing the arrangements.

large data providers would need to enter into 10 or fewer additional onboarding arrangements in the years immediately following implementation of the rule, at a maximum cost of $68,000 per large data provider.[159] In contrast, medium sized entities are likely to rely on core banking providers or other vendors to facilitate onboarding on their behalf at minimal incremental cost. Over time, data providers are likely to enter into additional onboarding arrangements due to entry by new third parties and other changes in the market.[160]

The CFPB requested comment on how the proposed rule would change both the cost of onboarding third parties and the number of data access arrangements between data providers and third parties. A bank, a credit union, and two research institutes commented that the costs to vet third parties will be substantial, with the bank and credit union further asserting the CFPB has underestimated those costs. A nondepository entity trade association commented that there will be an increase in costs stemming from the increase in the number of data agreements caused by the rule. Another credit union asserted that small credit unions do not have the necessary legal resources to vet third parties. Two banks asserted that the CFPB underestimated the costs of negotiating connection agreements. In contrast, a data aggregator estimated that the rule will reduce the cost of these agreements by at least 30 percent.

The CFPB acknowledges that data providers may incur costs associated with vetting third parties but expects that consensus standards will eventually develop around the rule's requirements and the ways that third parties can demonstrate compliance, which will mitigate

[159] This estimate was derived from the $6,800 estimate from the proposal for the cost of establishing a data access agreement multiplied by the up to 10 additional agreements that may need to be established due to the rule.

[160] For example, this final rule and the Industry Standard-Setting Rule aim to accelerate the development and adoption of consensus standards covering myriad aspects of open banking. This would likely reduce the frictions and costs associated with establishing and maintaining connections between data providers and third parties, potentially increasing the number of access agreements negotiated by data providers but reducing the costs of each agreement.

costs for data providers by putting the onus on third parties to show they are credible and secure. Furthermore, the CFPB expects that data aggregators will continue to act as intermediaries between data providers and third parties over the short to medium term, which will reduce the costs to data providers of onboarding additional third parties to compliant developer interfaces. However, based on the information provided by commenters, the CFPB is increasing its estimate of the number of hours required to finalize an onboarding arrangement from 80 hours to 120 hours on average, representing an average cost per agreement of $10,800.[161] Given the CFPB's expectation that large data providers would need to enter into 10 or fewer additional onboarding arrangements in the years immediately following implementation of the rule, the CFPB estimates a maximum cost of $108,000 per large data provider.[162]

Prohibition on fees for access

The rule does not permit data providers to charge fees for access to covered data through their interfaces. To the limited extent that data providers are currently charging such fees, the rule would eliminate these revenues. Based on the Aggregator Collection, the Provider Collection, and its market research, the CFPB understands that fees for consumer and third party access are currently rare.

The CFPB understands that third parties have in some cases made payments to data providers to incentivize data providers that are reluctant or unable to provide a developer

[161] This estimate was derived from BLS data showing a mean hourly wage for compliance officers ($38.55), general and operations managers ($62.18), lawyers ($84.84), and software developers ($66.40), for an average hourly wage of $62.99. BLS data also show that wages account for 70 percent of total compensation for private industry workers, leading to an $89.99 estimate for total hourly compensation, which was multiplied by the expected total number of hours of work required.

[162] This estimate was derived from the $10,800 estimate for the cost of establishing a data access agreement multiplied by the up to 10 additional agreements that may need to be established due to the rule.

interface of sufficient quality sufficiently quickly. While rare in the current market, the rule eliminates such fees that might have been charged in the future under the baseline.

The CFPB does not have representative data on the prevalence or size of payments to data providers and therefore cannot precisely estimate the cost of eliminating them. However, as described above, the information available to the CFPB indicates that few data providers currently charge third parties for access and that the total cost to data providers of eliminating such charges would be minimal.

The CFPB received many comments on the costs associated with the prohibition of fees. Many banks, credit unions, and bank or credit union trade associations commented that the prohibition of fees means that data providers will not be able to recoup the costs of complying with the rule. One trade association and a bank asserted that the CFPB has failed to fully consider the costs associated with a prohibition of fees but did not provide additional information upon which to base updated estimates. SBA Advocacy suggested that the CFPB could allow small entities to charge fees to recoup costs.

The CFPB acknowledges that covered data providers that would charge fees for receiving requests or making available consumer-authorized covered data to third parties under the baseline will not be able to do so under the rule, including to establish or maintain interfaces required under the rule. The prohibition on fees for data access would be costly for such covered data providers. The information available to the CFPB indicates that few, if any, covered data providers currently charge these fees or would charge these fees in the future under the baseline.

The CFPB acknowledges that covered data providers will incur costs associated with the rule and may seek new sources of revenue to offset those costs. The prohibition on fees for data access forecloses one possible new source of revenue. However, to the extent that covered data

providers would charge these fees in order to pass some compliance costs through to other market participants, these costs are appropriately accounted for in the discussion of these costs. Under an alternative where there is no fee prohibition, some covered data providers would likely require third parties or consumers to pay fees in order to access consumer-authorized covered data. As few, if any, covered data providers currently charge these fees, the CFPB cannot anticipate with certainty how common fees would be if permitted, which data providers would be most likely to charge fees, or how these fees would be set in equilibrium. In general, covered data providers would benefit from the option to charge fees. If fees were charged directly to consumers, consumers would incur the cost of paying the fees or the cost of forgoing the benefits of products and services enabled by consumer-authorized covered data. To the extent that consumers would not exercise their right to access their covered data due to fees, third parties would also incur costs related to a smaller potential market for their products and services. If fees were instead charged to third parties, third parties would incur the direct cost of paying the fees. Third parties would likely pass through some of those fees on to consumers. Depending on how they were structured, fees would change third parties' incentives in ways that might limit consumers ability to access third party products and services or degrade the quality of products and services. For example, if data providers charged fees based on the number of consumer accounts accessed, third parties would have an incentive to deter or deny less profitable consumers from using their product or service. As another example, if data providers charged fees for each access attempt, third parties would have an incentive to reduce the frequency with which they update consumer-authorized covered data, which would diminish the benefits to consumers of products and services that rely on real-time consumer data.

As discussed in part IV.C.2, the CFPB considered allowing fees for data access, but determined that the potential for data providers to set fees that are not reasonable and that inhibit consumers' access posed too great of a risk to the benefits of the rule as a whole. Further, small depositories, the institutions currently least able to absorb these costs and therefore potentially most likely to seek to offset them with new fees, are not required to comply with the rule's requirements on data providers.

More frequent access by third parties

Based on responses to the Provider Collection, the CFPB is aware that covered data providers sometimes impose access caps, such as limiting the number of allowable data requests or the frequency with which authorized third parties can access consumer data. For example, the CFPB is aware that some data providers cap the number of data requests per day per connection. The CFPB understands that in some cases access caps prevent third parties from accessing consumer data as often as is reasonably necessary to provide the requested service. For example, one firm in the Aggregator Collection reported spending "significant resources" to manage its traffic in order to avoid access cap limits. Another firm in the Aggregator Collection reported spending resources to persuade large financial institutions to raise or eliminate access caps. Therefore, the prohibition on unreasonably limiting the frequency of third party requests for covered data or delaying responses to those requests is likely to increase total data requests for some covered data providers and may therefore increase digital infrastructure costs for those data providers relative to the baseline.[163] This increase is likely to be larger for data providers with more restrictive access caps at baseline, if such access caps are not reasonable under the rule.

[163] As discussed in the section on *Benefits to data providers* in part VI.E.3, other features of the proposed rule are likely to decrease the frequency and scope of data requests and therefore digital infrastructure costs for covered data providers.

The CFPB expects that for most data providers, any increase in traffic due to such increases in the number of data requests will generally be more than offset by declines in screen scraping, which the CFPB understands to typically involve heavier traffic loads per request than requests through a developer interface. A small number of large data providers have already restricted screen scraping under the baseline and may experience net increases in developer interface traffic.

A bank trade association commented that a lack of access caps for developer interfaces would increase compliance costs and potentially degrade interface performance. As discussed in part IV.C.3., the CFPB has determined that data providers are permitted to impose reasonable access caps, to ensure that requests from one authorized third party do not unduly burden the data provider's developer interface. Given this determination, the CFPB expects that incremental costs from any increased data requests are likely to be minimal on a per-account basis.

Reduced information advantages

Through their role in providing financial products and services, data providers possess "first party" data on the accounts held by their customers. These data are a valuable source of information for data providers in developing, pricing, and marketing products and services, but authorized data access may reduce this information advantage. The CFPB expects that the rule will generally increase third party access relative to the baseline and thus diminish data providers' informational advantages from first party data. This may enable third parties to more effectively compete with products or services offered by data providers, potentially limiting the prices data providers can charge for their own products and services or reducing data providers' market shares or data providers' profits. For example, the CFPB understands that an important use case for consumer-authorized financial data is transaction-based underwriting. At baseline,

many data providers sell credit products to their depositors. To the extent that the rule facilitates entry into the lending market or improves the quality of the products and services offered by nondepository lenders or other depository lenders that use consumer-authorized data, data providers that enjoyed informational advantages relative to their peers may lose market share and therefore profits. As another example, consumer-authorized data sharing is likely to facilitate faster new account openings. As it becomes easier for consumers to compare account terms, transfer recurring payments, move funds, and have their identity verified, depository data providers may face pressure to pay higher deposit rates or make costly investments in service quality in order to retain deposits, as discussed in the section on *Benefits to consumers* in part VI.E.4.

In general, accurately predicting how changes in the availability of consumer-authorized financial data will change the structure of the market for consumer financial services or how changes in market structure will impact the profitability of individual firms or industries is very difficult, in large part because firms that are data providers in some cases also operate as third parties accessing data from other data providers, and the CFPB expects more data providers to act as third parties over time. As a result, the CFPB is not able to quantify the impacts of reduced informational advantages that stem from the proposal.

The rule is likely to increase the quality of services that use consumer-authorized financial data to facilitate competition, including by comparing or recommending products or services to consumers. This may impact data providers. For example, a consumer might use a comparison shopping service that would recommend credit cards likely to minimize their costs from interest and fees or maximize their benefits from rewards programs given their historical spending patterns. The CFPB is not able to accurately predict how many firms would develop

services that facilitate competition in this way, how many consumers would use such services, or how the availability of such services would impact individual firms or industries.

Many data providers and bank or credit union trade associations expressed concern that the rule would advantage third parties at the expense of data providers. A credit union trade association asserted that the CFPB did not properly assess the risks from the growth of non-bank lenders.

The CFPB notes that data providers may also act as third parties. Furthermore, the rule places substantial restrictions on how third parties can use and retain these data, relative to the baseline of screen scraping and no restrictions on the use or retention of the data. The CFPB acknowledges that there may be growth in nondepository lending but has determined that the rule's restrictions and existing regulations that apply to nondepository lenders under the baseline will mitigate the risks associated with this growth.

Potential costs related to liability or fraud

Several data providers and bank or credit union trade associations commented on the high costs of resolving disputes, dealing with third parties lacking appropriate security, and the costs of liability falling disproportionately on data providers. Two credit union trade associations expressed concern that, even when a third party is responsible for a data breach, data providers will face reputational risk, losses due to fraud, and costs to resolve the breach. The SBA Office of Advocacy commented that the lack of clarity in the rule regarding liability could lead to confusion and expensive litigation. A few data providers and a bank trade association asserted that the CFPB did not fully account for the costs associated with security breaches and liability. A few bank trade associations and data providers asserted that the absence of a ban on screen scraping will create costs for data providers to block screen scraping. The CFPB notes that these

risks exist under the baseline and are likely worse in the current marketplace, as discussed in the *Benefits to data providers* part, because of the widespread storage of credentials, the lack of rules on data retention, and downstream data sharing or sales by third parties. A credit union commented that they have already spent resources on increasing security and blocking screen scraping under the baseline. The CFPB expects that the allowance for reasonable denials in the rule and the role of consensus standards related to third party data security will also mitigate these risks by allowing data providers to deny access for third parties that have not established sufficient security protocols. The CFPB acknowledges that some institutions, especially those without developer interfaces, may face higher costs to develop and maintain data security systems, but the CFPB expects that the majority of data providers will see a net decrease in fraud risks and reputational risks relative to the baseline with widespread screen scraping and no restrictions on data collection, retention, and use.

Potential costs from increased account switching

In general, consumers prefer financial institutions that provide better prices or customer experiences. As discussed in the section on *Effects of increased data sharing on innovation and competition* in part VI.E.4, the CFPB expects that the rule will improve consumers' ability to switch financial institutions. As a result, financial institutions that offer covered products with less competitive prices and customer experiences may lose market share due to the rule. In addition, if greater competition on price leads to lower margins on covered accounts, profits for data providers that lower their margins in response to the rule will be decreased.

Costs to third parties

Third parties accessing data under the rule will be required to modify existing procedures, so they are consistent with the proposal's authorization procedures for accessing covered data on

behalf of a consumer, such as providing the authorization disclosure; implementing the limitations on data collection, use, and retention; developing mechanisms for revocation of authorization; providing the annual reauthorization of access; and executing record retention requirements. In addition to these upfront and ongoing compliance costs, the rule may impose further costs on third parties through the transition away from screen scraping access, increased data interface onboarding costs with data aggregators and data providers, restrictions on data use and retention. Potential effects of the new financial data processing products or services definition are also discussed.

Implementing mechanisms for data deletion and record retention

The rule requires third parties to establish and maintain systems that receive data access revocation requests, track duration-limited authorizations, and delete data when required due to revoked authorizations, durational periods ending, or because retaining the data is no longer reasonably necessary. Third parties will also need to retain records as required by the rule. Many of these requirements overlap with the requirements of other State or international data privacy laws. For example, third parties that operate in the State of California and have gross annual revenues greater than $25 million may already have similar systems if they are subject to the California Consumer Privacy Act (CCPA),[164] which requires that businesses delete consumer personal data upon consumer request. Though many State privacy laws exclude businesses or data covered by the GLBA, third parties that are regulated by State privacy laws may need to modify their systems, incorporate authorization duration limits, and process more revocation requests, but they will likely have lower costs than third parties that must establish such a system from scratch. The CFPB estimated in the SBREFA Panel Report, and described in the proposal,

[164] Cal. Civ. Code section 1798.198(a) (2018).

that establishing and maintaining an appropriate data system would cost up to $75,000 based on analysis of the Standardized Regulatory Impact Assessment for the CCPA.[165] The CFPB understands that some third parties already retain records related to consumer data access requests. The rule will require third parties to retain records that demonstrate compliance with the rule, including a copy of the authorization disclosure and, if a data aggregator accessed consumer-authorized data, a copy of the certification statement. The CFPB expects that the costs of implementing record retention requirements would be small relative to the costs of implementing deletion requirements.

As described in the SBREFA Panel Report, several small entity representatives provided cost estimates of implementing data retention limits. At the low end, one third party small entity representative that had implemented de-identification and deletion systems stated that it took between 240 and 480 hours of staff time,[166] and another third party small entity representative stated that it developed a system to comply with the CCPA in about 480 hours. At the high end, one third party small entity representative estimated that building a system to comply with retention limits would take 1,000 hours. If a third party chose not to establish a system to implement the retention limits of the rule and instead chose to manually delete data to comply with the retention limits, the CFPB understands that the time cost would be substantially higher: one third party small entity representative explained that, as an organization of fewer than 50

[165] The Standardized Regulatory Impact Assessment for the CCPA estimated that the average technology cost would be $75,000. However, the CFPB estimates that the cost for many third parties would be lower, as the CCPA figure was based on a survey of the top one percent of California businesses by size (those with more than 500 employees), and the CCPA has more requirements than the proposed rule. *See* Off. of the Att'y Gen., Cal. Dep't of Just., *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* (Aug. 2019), https://dof.ca.gov/wp-content/uploads/sites/352/Forecasting/Economics/Documents/CCPA_Regulations-SRIA-DOF.pdf.

[166] The small entity representative reported that the task took its team two to four weeks. Based on other small entity representative team sizes, the CFPB assumes that the team included three people.

people, complying with a single deletion request could require 480 hours. Based on this feedback, the CFPB estimates that the one-time cost of implementing data retention limits and retaining relevant records will be between $22,800 and $94,900.[167] The three-year record retention requirement of the rule will impose limited additional electronic storage costs annually.

One nondepository entity trade association commented that record retention requirements on third parties will impose far higher annual costs than estimated in the proposed rule, especially for smaller entities. The CFPB requested additional data or other information to further refine its estimates but did not receive cost estimates specific to revocation of authorization systems, implementing data retention limits, or record retention. The CFPB expects that the cost will be lower for third parties that already comply with existing data privacy laws. Third parties that do not retain any consumer-authorized data will be unaffected by data retention limits but will still need to follow record retention policies under the rule. The CFPB has determined that these record retention requirements are necessary to ensure compliance with the other components of the rule.

Annual reauthorization process

The rule limits the duration of third party collection of covered data to no more than one year after a consumer's most recent authorization. Third parties will be required to obtain a new authorization from the consumer before the first anniversary of the consumer's most recent authorization to continue to collect the consumer's covered data without disruption. Because this new authorization will have the same legal requirements as the first authorization, most of its implementation costs would be captured by the costs described for the initial authorization and

[167] The CFPB assumes that implementing deletion requirements would require between 240 and 1,000 hours of work by a software developer. The cost estimate was derived from BLS data showing a mean hourly wage for software developers of $66.40. BLS data also show that wages account for 70 percent of total compensation for private industry workers, leading to a $94.86 estimate for total hourly compensation.

data retention systems. The CFPB expects that reauthorization reminders will typically be delivered electronically—such as a within-app notification or an email—at minimal additional direct cost.

The reauthorization and retention limits may limit the quantity of data available for product improvement or other permissible uses of data. Some third parties may experience indirect costs due to service disruptions if they do not obtain a new authorization from the consumer before the anniversary of the consumer's most recent authorization, as they would not be able to request the consumer's data from data providers until the new authorization was obtained if more than one year has passed since the most recent authorization. If the consumer provides a new authorization after one year, any gaps in the scope of data collected would likely be filled, as the third party could then access two years of retrospective data.

The costs associated with the reauthorization requirement will depend on the third party's business model. Two small entity representatives suggested in the SBREFA process that periodic reauthorization requirements on third parties could lead to reduced customer retention. One small entity representative stated that this would "frustrate" consumers, and another stated that only 0.32 percent of its users prompted to reconnect to their bank account ever did so. A nondepository entity trade association commented that annual reauthorization would limit the value of pay-by-bank use cases, especially for recurring payments, and noted that card payments are not subject to reauthorization requirements. However, the CFPB understands that consumers are often required to reenter their card information for reoccurring payments after a card is lost, stolen, or expired, so consumers are not unfamiliar with reauthorizing payment methods.

Studies indicate that onerous reauthorization requirements have impacted open banking usage and attrition in other countries. Reauthorization requirements created friction for third

parties in the United Kingdom's open banking regime after the implementation of a 90-day reauthorization requirement. One United Kingdom trade association estimated an attrition rate between 20 percent and 40 percent, while another trade association found an attrition rate between 35 percent and 87 percent.[168] These attrition rates are likely to be different than those expected under the rule both because a 90-day reauthorization requirement is more burdensome than an annual reauthorization requirement and because more consumers may still be actively using a product or service after 90 days than after one year. The CFPB expects that, while some third parties would incur costs from consumer attrition, third parties will be more likely to obtain a new authorization from a consumer when that relationship is more valuable, and the reauthorization process will be relatively easy for consumers who wish to continue the relationship. These factors will generally limit the cost of disruptions due to the reauthorization requirements, particularly for third parties providing the most valuable services. The CFPB does not have data to estimate the costs to third parties of lost customers due to the annual reauthorization requirements.

Providing authorization disclosure and certification statement

The rule requires third parties to provide the authorization disclosure and certification statement when seeking to access covered data. When a third party seeking authorization uses a data aggregator to assist with accessing covered data on behalf of a consumer, the rule requires the data aggregator to make its own certification statement to the consumer, though both the aggregator and third party certifications will be permitted to be made in the same disclosure. The CFPB expects that some data aggregators will provide the required authorization disclosure and

[168] *See* Fin. Conduct Auth., *Changes to the SCA-RTS and to the guidance in 'Payment Services and Electronic Money—Our Approach' and the Perimeter Guidance Manual* (Nov. 2021), https://www.fca.org.uk/publication/policy/ps21-19.pdf.

certification statement on behalf of third parties seeking authorization. However, some third parties seeking authorization, including those that do not partner with data aggregators, may instead provide the authorization disclosure and certification statement through their own systems.

For data aggregators and other third parties that choose to provide the authorization disclosure and certification statement through their own systems, and have not previously provided any disclosure statements to consumers, the CFPB estimates that building such a system would require approximately 1,000 hours of work by software developers or similar staff. This estimate is based on cost estimates in other consumer financial markets related to requirements for tailored disclosures provided at service initiation.[169] The CFPB estimates that this will result in a one-time cost for a third party of $94,900.[170] However, if third parties already provide disclosures at authorization under the baseline, the costs of modifying these disclosures to satisfy the proposal's requirements may be reduced. One data aggregator stakeholder stated that modifying the content of its existing disclosures would involve 30 to 40 hours of employee time, representing an equivalent cost for a third party of between $2,900 and $3,800.[171]

Data aggregators may pass through these costs to third parties that contract with them. One data aggregator stated in its response to the Aggregator Collection that disclosures for third parties that contract with data aggregators would be largely uniform and easily adapted, and the

[169] 82 FR 54472, 54823 (Nov. 17, 2017).

[170] This estimate was derived from BLS data showing a mean hourly wage for software developers of $66.40. BLS data also show that wages account for 70 percent of total compensation for private industry workers, leading to a $94.86 estimate for total hourly compensation, which was multiplied by the expected total number of hours of work required.

[171] This estimate was derived from BLS data showing a mean hourly wage for software developers of $66.40. BLS data also show that wages account for 70 percent of total compensation for private industry workers, leading to a $94.86 estimate for total hourly compensation, which was multiplied by the expected total number of hours of work required.

CFPB anticipates that this will be the case under the rule. The CFPB does not have data to estimate these disclosure costs. However, because data aggregators' disclosure costs would be spread across many third parties, the CFPB expects the burden of these requirements on any single third party that contracts with data aggregators to be small.

Policies and procedures

To implement the requirements of the rule, third parties will need to develop and maintain policies and procedures in several distinct areas to ensure compliance with the rule. These include: applying existing information security programs to their systems for the collection, use, and retention of covered data; ensuring the accuracy of the information that they collect; governing the limits on collection, use, and retention of consumer-authorized information; and record retention requirements. The CFPB understands that most authorized third parties and data aggregators are currently subject to the GLBA Safeguards Framework and so they already have policies and procedures regarding information security programs and will have lower costs for developing and maintaining similar requirements of the rule. However, a small portion of third parties may need to develop new GLBA-compliant systems and would face greater costs. In other consumer financial markets, the CFPB has estimated that nondepository institutions would face a one-time cost of $5,300 to develop new policies and procedures and a one-time cost of $4,800 for a legal/compliance review.[172] Assuming comparable costs for the requirements of the rule yields a total cost of roughly $10,100 for developing and implementing policies and procedures. Maintaining these policies and procedures once they are implemented is likely to involve limited ongoing costs for third parties.[173]

[172] Inflation-adjusted estimates from 88 FR 35150 (May 31, 2023).

[173] SBREFA Panel Report at 12.

Transition away from screen scraping

The CFPB expects that third parties may face costs from the transition away from screen scraping. At baseline, screen scraping is a frequently used method of accessing consumer data: in 2022, roughly half of data access attempts by third parties in the Aggregator Collection were made through screen scraping. However, the share of access attempts made through screen scraping declined by approximately one-third between 2019 and 2022. The CFPB expects that screen scraping will continue to decline for non-covered financial products as data providers and third parties generally transition to data access under the terms of the rule. The CFPB expects that third parties will have strong incentives to avoid using screen scraping to access covered data from data providers that have compliant interfaces for third parties. In the SBREFA process, multiple small entity representatives expressed that the transition away from screen scraping would limit data accessibility. Relative to the baseline, the CFPB does not expect the transition away from screen scraping to negatively impact data availability for most data fields. The CFPB expects that data providers that provide third party access in compliance with rule requirements will block screen scraping for covered accounts, so third parties may not be able to access non-covered data fields from covered accounts. The CFPB requested comment on any specific data fields that may be less available due to the transition away from screen scraping, and the specific impacts of those changes, but did not receive relevant comments. The CFPB expects that the rule will not directly impact how third parties access non-covered data.

At baseline, some third parties use screen scraping as a back-up access method when other data access systems are inoperable. The need for a back-up access method may be reduced under the rule because the rule imposes performance requirements for third party access. However, nondepository entity and researcher commenters expressed concern that these

requirements could still reduce the quality of information provided and drive a market-wide race to the bottom, contending that data providers would have little incentive to drive performance higher. These commenters asserted that the proposal's performance requirements might permit lower performance than in their extant data access agreements with data providers. However, the rule would impose a general reasonableness requirement in addition to minimum performance requirements. Because data providers cannot only meet the minimum performance requirements, and instead must additionally demonstrate reasonable performance, indicia of which include performance comparable to other data providers, the CFPB expects there would be upward pressure on performance levels over time. Additionally, a third party small entity representative stated in the SBREFA process that its customers lose access to services when data providers' interfaces are unavailable. The CFPB expects that consensus standards regarding performance, which also can serve as indicia of commercially reasonable performance, will also help improve the reliability of access over time. Furthermore, the value of screen scraping as an alternative option may be limited by its relatively low success rates: in the Aggregator Collection, 40 percent of initial account connection attempts made through screen scraping were successful in 2022, compared to 51 percent of initial account connection attempts made through interfaces for third parties. The CFPB does not have data to quantify any net change in data access reliability stemming from the combination of reduced screen scraping and increased availability of interfaces for third parties. However, with respect to nondepository entity comments that the proposed 3,500 millisecond response time was too slow and vague, the final rule instead requires a proper response within a commercially reasonable time. The CFPB did not change other performance standards outlined in the proposed rule after considering nondepository entity

comments in conjunction with those from data provider commenters, detailed in the section on *Costs to data providers* in part VI.E.1.

Cost of onboarding arrangements with authorized third parties and data providers

Third parties that previously accessed covered data through screen scraping without negotiating the terms of their access with data providers will now need to arrange for onboarding to the newly required developer interfaces. The CFPB expects that many of these arrangements will be established between data aggregators and data providers, though some would occur between authorized third parties that do not contract with data aggregators and data providers. As described in the section on *Costs to data providers* in part VI.E.1, the CFPB has updated its estimate of the average cost of this process between data aggregators and data providers to $10,800.

Third parties may be denied data access based on risk management concerns or other permissible grounds, such as, for example, if the requested information is not covered data or falls into an exception. The CFPB expects that third parties may incur costs from responding to data providers' risk management information requests. Two research institutes stated that third parties would incur costs from responding to data providers' due diligence requests. Because prudential regulators require banks to follow certain risk management practices in contracting with third parties, the CFPB understands that authorized third parties that contract with either a data aggregator or a data provider at baseline provide due diligence information and will not face increased costs under the proposed rule. Third parties that comply with the GLBA Safeguards Framework are also unlikely to face increased costs. Though third parties that access consumer data solely through screen scraping at baseline will need to begin providing this information to the entities with which they contract, the CFPB expects that future consensus standards may

limit the costs for third parties. The CFPB expects that third parties that comply with data providers' due diligence requirements will not be denied access to data providers' interfaces and so very few third parties would incur costs related to the loss of access entirely.

Use of TANs

Under the rule, data providers will be permitted to make available a TAN instead of, or in addition to, a non-tokenized account number. Several nondepository entity and data aggregator commenters provided examples of TANs enabling consumer payment revocation and stated that the use of TANs could increase costs for merchants and processers, which could be at least in part passed through to consumers. One nondepository entity estimated that the payments industry could face cumulative annual losses in the hundreds of millions of dollars if TANs were permitted under the rule. However, other data provider commenters described how TANs can mitigate fraud risk, including the ability for data providers to identify the point of compromise in case of a breach, the ability to revoke compromised payment credentials without disrupting other payment account activity, and limited risk of bank fraud because TANs are restricted to a particular third party.

Restrictions on use and retention

The rule limits certain existing uses of both identifiable and de-identified consumer data by third parties, including for the sale of covered data, cross-selling of other products or services, and targeted advertising, by specifying that these activities are not part of, or reasonably necessary to provide, any other product or service. Therefore, consumers must separately authorize third parties to collect, use, and retain covered data for these activities. This limitation may eliminate or lessen the profitability of certain business models. Third parties that generate revenue from sharing covered data with fourth parties—such as firms with no authorization to

access data from the consumer—may lose much of that source of revenue. The CFPB does not have data on the number of third parties that share covered data, or the amount of revenue generated by sharing covered data. However, the CFPB notes that a survey of German app developers after the European General Data Protection Regulation (GDPR) was implemented found that while the share of app developers selling data was small, nearly all the developers that sold data experienced a decline in revenue post-GDPR.[174] This finding may imply reductions in revenue for third parties that sell covered data under the rule. Several nondepository entity trade association commenters stated that small and mid-size businesses rely on targeted advertising and will lose revenue due to the proposed rule. Third parties that use covered data for the marketing of other products and services may also lose a source of revenue. Commenters did not provide quantitative data on the expected scope of potential revenue losses. The CFPB acknowledges that third parties may incur costs from altering business practices, or may lose revenue, as a result of these limitations. The CFPB does not have the necessary information to quantify this impact, but expects the overall impact on third parties will be small, as most third parties' revenue streams are not dependent on using covered data for these activities. Furthermore, third parties can still seek consumer authorization for covered data to be used for these activities as standalone products or services, or first-party data could be used.

In addition to these specific requirements, third parties will be required to collect, use, and retain covered data only as reasonably necessary to provide the consumer's requested product or service under the rule. The limits on retention of consumer data when consumers submit a revocation request or do not provide a new authorization within 12 months may reduce

[174] Rebecca Janßen *et al.*, *GDPR and the Lost Generation of Innovative Apps*, Nat'l Bureau of Econ. Rsch. Working Paper No. 30028 (May 2022), https://www.nber.org/papers/w30028.

the data available for product improvement. Several third party small entity representatives highlighted through the SBREFA process how consumer data can enable the development of new products and services and can inform research and public policy, even when only de-identified data are used for these secondary purposes. A nondepository entity trade association stated that there would be substantial costs to rework algorithms and product operations, which could not be used in their current form without de-identified consumer data. Firms in the Aggregator Collection also reported using consumer data for functions other than transmitting data to data recipients, including the improvement of existing products, the development of new products, and risk management assessments. One nondepository entity commented that using properly de-identified or aggregated data for modeling or developing new products leads to no harm to consumers. Several commenters, including nondepository entities, nondepository entity trade associations, research institutes, data aggregators, and data providers commented that secondary use restrictions would reduce competition and innovation under the proposed rule. One research institute commented that current models and algorithms would become stagnant and could not be further improved without the use of covered data. Multiple research institutes and a consumer advocate commented that disallowing the use of de-identified data for product development would result in more expensive and less innovative products. Additionally, multiple data aggregators commented that the inability to use de-identified data would limit the ability to detect fraud.

Though the rule may limit third parties' use of consumers' covered data for some extant purposes, the CFPB does not have data that would allow it to estimate the size of any costs due to the limitations on use, but notes that the rule permits uses that have separate product authorizations, and permits uses that are reasonably necessary to protect against or prevent fraud.

The rule also allows the use of covered data for servicing or processing the product or service authorized by the consumer, or uses that are reasonably necessary for the improvement of the consumer's requested product or service, without a separate product authorization.

Costs may be mitigated because third parties can continue to use data that they generate in providing their products and services. One bank trade association commented that there would be costs to tracking which data are subject to secondary use restrictions and which data are not. The CFPB acknowledges there could be such costs, but expects that these tracking costs would be small given that all consumer-authorized covered data would be subject to secondary use restrictions, and all first-party data would not be subject to secondary use restrictions under the final rule. The cost estimates in the section on *Implementing mechanisms for data deletion and record retention* in part VI.E.1 would include such costs.

New financial data processing products or services definition

The CFPB expects that the activities covered by the new financial data processing products or services definition in 12 CFR part 1001 are already within the scope of the CFPA's definition of financial product or service. As a result, the CFPB does not expect the new definition to impose costs on covered persons. However, to the extent that there are firms offering products or services that are within the new definition but outside of the existing financial product or service definition, the new definition could impose some potential costs. Such firms would be subject to the CFPA and its prohibition on unfair, deceptive, or abusive acts or practices, including potential enforcement by the CFPB. Under the baseline, the CFPB expects that such firms would already be subject to a prohibition on unfair or deceptive acts or practices under section 5 the Federal Trade Commission Act.[175] Relative to the baseline, the new

[175] 15 U.S.C. 45.

definition would add potential enforcement against unfair and deceptive acts or practices by the CFPB and require firms to be compliant with the prohibition on abusive acts or practices. Given the overlap with existing prohibitions, the CFPB expects the potential costs would be limited, and would include developing and maintaining policies and procedures to ensure compliance with the prohibition on abusive practices for firms that are not compliant with the CFPA at baseline. The CFPB does not have data to quantify these potential costs. The CFPB requested comment on whether any firms offer products or services that would be covered by the new definition but fall outside the definition of financial product or service, and if so, what potential costs those firms may face, but the CFPB did not receive any comments with this information.

2. Costs to consumers

The rule may increase costs for data providers and third parties, potentially leading to higher prices for consumers or reduced access to certain products or services. The rule is likely to increase the availability of consumer-authorized data overall. While this may benefit many consumers, it could lead to higher credit costs for some consumers with data indicative of higher risk if the use of this data becomes standard for underwriting purposes. The rule would also require consumers to reauthorize access to their financial data annually, which involves relatively minor costs. In addition, consumers may incur small costs because of unintentional lapses in authorization. Finally, restrictions on secondary use of data may reduce revenues for some third parties, leading to changes in product offerings or pricing, and limiting not-for-profit research analyses that may benefit consumers.

Changes in industry structure

Data providers will face additional compliance costs as a result of the rule. Some of these costs may be passed on to consumers in the form of higher prices for credit, lower deposit rates,

or higher account fees. The CFPB does not have the data necessary to determine the extent to which additional compliance costs may be passed through to consumers, which depends on a number of factors including market competition.

The rule does not require depository data providers that have assets below size standards specified by the Small Business Administration, which are currently set at $850 million, to comply with Subparts B and C. Several data provider commenters and trade associations representing them, along with a nondepository entity trade association and a consumer advocate commented that the rule may lead to consolidation among depository institutions, which may lead to higher prices and less choice for consumers. One credit union commented that costs relative to net income would force about half of credit unions to cease operations. The CFPB expects that the noncoverage of depository entities with assets below $850 million addresses the concern that small depository institutions would be unable to operate profitably and in compliance with the rule. For example, the median credit union in 2024 had $57 million in assets and would thus not be covered by the data provider provisions of the rule, and overall, 89 percent of credit unions are below the coverage threshold. While it is possible that the rule could influence decisions about consolidation for some institutions above the coverage threshold, the CFPB expects any effect to be small given the relatively large size of covered institutions. The CFPB did not receive any other data in comments that allows for a more precise estimation of whether institutions would choose to consolidate as a result of the rule.

Many of the largest depository data providers either already offer third party data access that meets many of the requirements of the rule or are developing such functionality, and thus their additional costs of complying with the rule will be more limited. While the CFPB does not have information to precisely estimate the number of consumers with accounts at such data

providers, the available data suggest that the number is large. The Provider Collection indicates that, as of 2022, at least 51 million consumers had connected accounts to third parties through credential-free interfaces. This count of 51 million consumers likely understates the true number of consumers who have such access for two reasons. First, it does not include the consumers at institutions in the Provider Collection who have access to, but have not yet connected to, this type of access functionality. Second, it does not include consumers at other institutions—not included in the Provider Collection—that have established interfaces for third party access that meet many of the requirements of the proposal. It could, however, count consumers more than once if they have an account at more than one institution included in the Provider Collection. Overall, the CFPB expects that substantially more than 51 million consumers already have accounts at institutions that will face more limited costs of complying with the provisions. Consumers who only have accounts at these institutions are likely to incur minimal costs passed on by data providers due to the rule because the institutions where they have accounts will face smaller costs. One credit union trade association commenter stated that the rule will accelerate a transition to digital services and reduce the number of branches, which some populations, such as older consumers, rely on. The CFPB does not have data to precisely analyze this claim but finds it unlikely that the rule will result in many branch closures. In 2023, only 9 percent of Americans said that they most often managed their bank account by visiting a branch.[176] Thus, the industry has already experienced a dramatic shift toward online services, and the margin for consumers to transition toward digital banking and cease visiting bank branches, leading to branch closures that affect older consumers, is small. Since the CFPB expects that all or nearly all covered data

[176] Press Release, Am. Bankers Ass'n, *National Survey: Bank Customers Use Mobile Apps More Than Any Other Channel to Manage Their Accounts* (Oct. 26, 2023), https://www.aba.com/about-us/press-room/press-releases/consumer-survey-banking-methods-2023.

providers already have a consumer interface, it is likely that consumers interested in online services already conduct much of their banking online. Despite few consumers preferring to manage an account by visiting a branch, the number of bank branches nationwide has declined only 16 percent from its peak in 2012 and actually grew slightly between 2022 and 2023.[177] Further, branches serve small businesses in addition to consumers, so are not supported by consumers alone.[178] A credit union trade association commented that financial institutions could be discouraged from adopting a consumer interface if they do not already have one because of the costs associated with the proposed rule. As discussed in part IV.A.3., the CFPB has determined that all or nearly all depositories that do not currently have a consumer interface are small depository institutions and therefore will not be required to comply with the final rule's requirements for data providers. In addition, coverage in the final rule is no longer determined by the presence of a consumer interface, and thus there is no disincentive to adopt a consumer interface created by the final rule.

Effects of greater information sharing

The rule will enhance third party access to consumers' financial data, which may be used in third parties' credit underwriting decisions. The ability for firms to screen customers using information generally increases total value in the market but may transfer value from some consumers to firms. Some consumers will likely benefit, but other consumers may be worse off. While the CFPB understands that, currently, lenders do not commonly use cash-flow data in

[177] *See* Fed. Deposit Ins. Corp., *BankFind Suite: Find Annual Historical Bank Data*, https://banks.data.fdic.gov/explore/historical/?displayFields=STNAME%2CTOTAL%2CBRANCHES%2CNew_Char&selectedEndDate=2023&selectedReport=CBS&selectedStartDate=1934&selectedStates=0&sortField=YEAR&sortOrder=desc (last visited Oct. 16, 2024).

[178] For example, Community Reinvestment Act data suggests that branches are important in small business lending. Elliot Anenberg *et al.*, *The Branch Puzzle: Why Are there Still Bank Branches?*, FEDS Notes (Aug. 20, 2018), https://www.federalreserve.gov/econres/notes/feds-notes/why-are-there-still-bank-branches-20180820.html.

underwriting to identify consumers who are a higher risk than the information on traditional credit reports would predict, it is possible that the market will evolve to use cash-flow data in this way as it becomes more accessible. As a benefit, increased information about consumers could lead lenders to offer some consumers cheaper credit, if, for example, the information accessed from data providers is viewed by third party lenders as indicating that the consumer is a lower credit risk than a traditional credit report would reveal. More information, however, could result in some consumers being charged higher prices or not being offered credit if the cash-flow information reveals what a lender views as a signal that a consumer is a higher credit risk than the lender would have assessed without the consumer-authorized information.[179] Even though it will be the consumer's choice whether to authorize access to their covered data, it is possible that a lender may view a consumer's decision not to authorize the sharing of their data as a negative signal of credit risk and raise the price of credit or refuse to offer a loan.[180]

[179] For example, Jansen *et al.* (2022) study an opposite shock—the removal of information, instead of the addition—and find that removing bankruptcy information from credit reports redistributes consumer surplus from consumers who have never experienced bankruptcy to consumers with a previous bankruptcy. Mark Jansen *et al.*, *Data and Welfare in Credit Markets* (Jan. 28, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4015958. Nelson (2023) finds that limiting the information that credit card issuers were able to use decreased prices for some high-risk borrowers and increased prices for some low-risk borrowers, but on aggregate raised consumer surplus. These are two examples of how the removal of information that can be used in crediting decisions may shift surplus towards consumers who appear to have lower repayment risk after the information removal. Scott T. Nelson, *Private Information and Price Regulation in the US Credit Card Market*, Univ. of Chic. Booth Sch. of Bus. (Aug. 4, 2023), https://faculty.chicagobooth.edu/-/media/faculty/scott-nelson/research/private-information-and-price-regulation-in-the-us.pdf. The CFPB expects that the following effects would occur under the rule: third parties will have access to more information which will increase total surplus and will likely increase surplus for those who appear to have lower repayment risk with the additional information relative to those who appear to have higher repayment risk with the additional information.

[180] He, Huang and Zhou (2023) develop a model in which consumers who choose not to share data are worse off under an open banking system due to lenders taking opting out of data sharing as a sign that a consumer is a high credit risk. Zhiguo He *et al.*, *Open banking: Credit market competition when borrowers own the data*, 147 J. Fin. Econ. 449 (2023), https://doi.org/10.1016/j.jfineco.2022.12.003. Similarly, Babina *et al.* (2023) develop a model showing that when open banking policies enable the addition of banking data to screening or pricing decisions, higher-cost consumers can be worse off even if they opt out of sharing information because opting out sends a negative signal to lenders. Tania Babina *et al.*, *Customer Data Access and Fintech Entry: Early Evidence from Open Banking*, Stanford Univ. Graduate Sch. of Bus. Rsch. Paper (Sept. 7, 2023), https://dx.doi.org/10.2139/ssrn.4071214.

Overall, the increased availability of consumer-authorized data will allow lenders to underwrite and price more efficiently. This will likely lead to greater credit access overall, with relatively greater access or lower prices for lower risk borrowers who share data, but relatively less credit access or higher prices for borrowers who are higher risk or choose not to share data. The CFPB does not have the data necessary to quantify these effects.

Time cost of reauthorizing third party access annually

Under the rule, a third party will need to limit the duration of collection of covered data to a maximum period of one year after the consumer's most recent authorization. To collect covered data beyond the one-year period, the third party will need to obtain a new authorization from the consumer no later than the anniversary of the consumer's most recent authorization. The reauthorization process should not be more burdensome than the initial authorization certification, but consumers will incur a small time cost to reauthorize the collection of their data. As discussed in the section on *Costs to third parties* in part VI.E.1 above, existing evidence suggests that many consumers may choose not to reauthorize a third party's access to their covered data. The CFPB interprets this evidence as suggesting that many consumers do not value the continued use of the third party product or service enough to continue authorizing the access of their covered data by the third party or that, given the quickly evolving market of third party products and services, consumers decide to access products or services through a different third party. One nondepository entity trade association commenter stated that the annual reauthorization limits the utility of pay-by-bank use cases for consumers. Instead, the CFPB interprets a consumer's decision to not provide a new authorization as evidence that they do not value the service more than the relatively small time cost incurred to reauthorize access. Further, consumers who currently pay by credit or debit card may face a similar reauthorization cost

when a card expires or is replaced due to fraud, so these types of costs are not unique to the pay-by-bank model.

Potential changes in pricing models due to use and retention limitations

Changes that third parties make to their business models as a result of the rule may be passed on to consumers through higher prices for services provided by third parties. For example, the CFPB understands that some third parties obtain revenue by selling data that consumers provide to them with other third parties or, more commonly, by selling marketing information derived from such data. This may allow third parties to provide services to consumers free of charge. As discussed in the *Costs to third parties* part, there is evidence that firms in Europe that were sharing customers' data experienced a decline in revenue after data protection laws were enacted, suggesting that they may need to seek alternative sources of revenue.[181]

The CFPB expects that the rule will reduce the amount of targeted advertising using covered data. Several nondepository entity trade association commenters stated that consumers benefit from targeted advertising and prefer ad-supported services to fee-based services, and so the prohibition of the use of covered data for targeted advertising under the rule will harm consumers. But this overlooks that the rule does not prohibit targeted advertising. Providers can still use other forms of data for this purpose. And they can use covered data for this purpose, so long as they do so in the form of a standalone product or service, consistent with the terms of the rule. To the extent consumers benefit from targeted advertising, the rule provides means to realize such benefits.

[181] Rebecca Janßen *et al.*, *GDPR and the Lost Generation of Innovative Apps*, Nat'l Bureau of Econ. Rsch. Working Paper No. 30028 (May 2022), https://www.nber.org/papers/w30028.

To the extent that the rule leads to third parties changing their business models, it is possible that some third parties will charge consumers directly for services that used to be free. The CFPB does not have data to estimate the share of consumers impacted or the magnitude of any corresponding price increases.

Reduction in not-for-profit research analyses

Multiple research institutes and researchers commented that restrictions on secondary uses of consumer data would eliminate the use of open banking data in not-for-profit research analyses, which may harm consumers. Research institutes and researchers considered the possibility of an "opt-in" option for consumers to choose to share their covered data for the purpose of not-for-profit research, but expressed that research limited to this population would not generally be representative and therefore would be of limited value. These commenters requested an exception that would permit non-commercial secondary uses for de-identified data. The CFPB acknowledges that the rule will likely reduce the availability of consumer-permissioned data for nonprofit research purposes, and that this could have some indirect costs for consumers. The CFPB does not have data or evidence that would allow it to quantify these potential indirect costs.

3. Benefits to covered persons

Benefits to data providers

At baseline, many third parties use screen scraping to access consumer data. The CFPB expects that screen scraping will decline under the rule. This is likely to benefit data providers because screen scraping involves security risks and heavy web traffic. By standardizing the terms of access and reducing the scope of negotiation, the rule is also likely to decrease the per-arrangement cost of enabling access to the developer interface. Finally, data providers that

provide competitive service offerings, including potentially community banks and credit unions, could benefit from increased account switching by consumers.

Reduced screen scraping

The CFPB understands that credential-based screen scraping creates data security, fraud, and liability risks for data providers, particularly because the credentials shared to facilitate data access also typically can be used to move funds. Furthermore, screen scraping can be used to gather data without data providers establishing a relationship with third parties or assessing data security risks. The CFPB cannot disaggregate fraud costs resulting from credential-based screen scraping from general costs of fraud, including measures to prevent fraud or insure against fraud-related damages. However, depository data providers have reported extensive costs related to preventing fraud and unauthorized transactions generally, and reimbursing consumers when such fraud occurs. During the SBREFA process, one small depository institution reported debit card fraud losses of 28 percent of their total revenue. Small entity representatives also noted that data providers typically pay premiums for insurance against catastrophic fraud losses, with plans typically covering losses in excess of $25,000, subject to certain restrictions. Through conversations with industry participants, the CFPB understands that account takeover fraud is the most likely fraud risk that could be exacerbated by credential-based data access methods such as screen scraping.[182] In this form of fraud, the bad actor gains access to the consumer's account and transfers funds, makes purchases, or opens accounts without authorization. The CFPB expects that the reduction in credential-based access due to the rule would lower the risk of account takeover fraud, providing a benefit to data providers through reductions in direct liability

[182] For example, consumers' account credentials may not be securely stored by third parties or fraudsters may induce consumers to share their credentials by impersonating a legitimate third party.

and decreased fraud insurance premiums, although it is unclear how much account takeover fraud is attributed to credential-based screen scraping. The CFPB does not have sufficient data to estimate how much the rule will lower account takeover fraud risk. However, even a small reduction would have large benefits for data providers.[183]

Along with the requirements to access only the data fields necessary to provide the specific product or service, the shift away from credential-based screen scraping will also tend to reduce overall traffic loads on the consumer-facing system and may reduce traffic loads overall. The CFPB does not have systematic data with which to estimate the net change in web traffic and the resulting decrease in necessary expenditures on digital infrastructure. The CFPB understands that the incremental cost of additional web traffic is small, and that reasonably anticipated reductions in traffic are likely to provide minimal benefits to data providers. In a comment, a data aggregator concurred with the CFPB that transitioning to developer interfaces should generally reduce the number of data requests and traffic relative to screen scraping, thus reducing costs for data providers.

Reduced onboarding costs and more standardized terms of access

The CFPB understands that onboarding third parties is often resource intensive for data providers. In the Aggregator Collection responses, aggregators reported that negotiating an access agreement with a data provider could take between 50 and 4,950 staff hours of business relationship managers, software developers, lawyers, compliance professionals, and senior management, depending on the complexity of the negotiation. The median estimated time was 385 staff hours per agreement. Based on these responses, under the baseline the CFPB estimated

[183] For example, a 3 percent reduction in ATO fraud risks would generate an expected annual benefit of $330 million for data providers, based on industry research finding ATO fraud risks of approximately $11 billion annually. *See* PaymentsJournal, *Javelin's Identity Fraud Study Highlights the Changing Nature of Fraud* (May 24, 2023), https://www.paymentsjournal.com/javelins-identity-fraud-study-highlights-the-changing-nature-of-fraud/.

a total cost of between $4,260 and $422,000, which varies depending on the complexity of the negotiation, with a median cost of around $32,825. Although these estimates were provided by data aggregators, the CFPB expects that these costs are also representative for data providers at baseline.

For contract negotiations that would have occurred under the baseline, the CFPB expects that onboarding costs will decrease under the rule because many features of access agreements would be regulated by the rule and not subject to commercial negotiation, including requirements for interface reliability, interface queries, and the scope of data accessible via the interface. One market participant stated that in cases where data providers agree to use existing industry-defined standards there is essentially no need for negotiation and data providers can immediately begin updating their developer interfaces in line with the standard specifications. The CFPB expects that consensus standards will reduce onboarding costs in this way. The CFPB expects that under the rule nearly all data providers will use standardized onboarding arrangements that meet rule terms and the costs of establishing data access will be limited to ensuring third party risk management standards are satisfied and reviewing the arrangements. A non-small entity representative third party commenter stated that concluding this type of onboarding arrangement represents approximately 20 percent of total negotiation time under the baseline.[184] Based on this, the CFPB estimated in the proposal that negotiations under the rule would require roughly 80 staff hours on average. The required time to onboard third parties to developer interfaces may decline substantially over time as consensus standards are developed for certifying compliance with third party risk management standards. While some data providers and third parties may choose to enter into customized access arrangements that respect the terms of the rule, they will

[184] *See* https://www.regulations.gov/comment/CFPB-2023-0011-0042.

generally only do so when the perceived benefits exceed the costs described here. As discussed in the section on *Costs to data providers* in part VI.E.1 above, commenters stated that the CFPB had underestimated the costs of establishing data access arrangements. In response to the information in these comments, the CFPB is updating its estimate to 120 staff hours on average to onboard a third party to a developer interface. Therefore, the CFPB estimates that the rule is likely to reduce the cost of onboarding arrangements by $24,000 on average.[185] Under the baseline, data providers would have continued to negotiate commercial access agreements with third parties and these benefits would not have applied to those agreements. As discussed in the section on *Costs to data providers* in part VI.E.1 above, the CFPB expects that the rule will cause data providers to onboard additional third parties relative to baseline. The cost of additional onboarding arrangements is analyzed in that part.

Restrictions on third parties' use and retention of data

The rule will also have some indirect effects on the value of first party data held by data providers. Under the baseline, third and first party data are both used for marketing and new product development.[186] The rule will limit third party collection of consumer-authorized data to what is reasonably necessary to provide the consumer's requested product or service. Third party use and retention of covered data will also be subject to that limitation, which will limit the availability of covered data for marketing and for the development of new products outside the scope of the original authorization, to the extent that third parties cannot obtain or use data for these purposes through other means. While the CFPB does not have data to quantify the benefits

[185] This estimate is based on estimated total hourly compensation of $89.99 multiplied by the difference between the median expected hours required at baseline, 385 hours, and the expected hours required under the rule, 120 hours.

[186] For example, a firm might target advertising towards consumers who qualify for a particular credit product or who are likely to be particularly profitable customers or develop new products based on insights from a dataset of consumer transaction histories.

to data providers, all else equal, this is likely to increase the value of first party covered data held by data providers, which generally does not have these restrictions.

Required data security representations by third parties

The rule will require authorized third parties to represent that they have reasonable security practices, in particular by representing that they implement the GLBA Safeguards Framework. These practices are likely to benefit data providers by increasing certainty regarding their potential third party risks, and generally will require minimum data security standards among third parties. The CFPB expects this to generally reduce the likelihood of data security breaches or other incidents, but the CFPB does not have data to quantify the size of this benefit.

Potential benefits from increased account switching

In general, consumers prefer financial institutions that provide better prices or customer experiences. As discussed in the section on *Effects of increased data sharing on innovation and competition* in part VI.E.4, the CFPB expects that the rule will improve consumers' ability to switch financial institutions. As a result, financial institutions that offer covered products with competitive prices and customer experiences may increase their market share due to the rule. This could particularly benefit community banks or credit unions that operate at a smaller scale and thus would have had comparatively smaller informational advantages relative to larger data providers under the baseline, as discussed in the section on *Reduced informational advantages* in part VI.E.1.

Benefits to third parties

Right to access data on behalf of consumers

Under the rule, covered data providers are required to provide data to authorized third parties. Third parties will be able to access data from data providers that had not made data

available under the baseline. Further, the rule's data reliability requirements will ensure that data access is consistently available across all data providers. The CFPB understands that, at baseline, connectivity failure rates between third parties and data providers are high, in part because many data providers do not facilitate data sharing with many third parties, so these requirements may lead to large increases in the proportion of consumers who are successfully able to share their data under the rule. Firms in the Aggregator Collection reported initial connectivity failure rates ranging from 28 percent up to 60 percent. The CFPB understands that some of these initial connectivity failure rates occur because the data provider denies the third party's request for data access, rather than because of low interface reliability, and so third parties will be able to reach more consumers under the rule's requirement that authorized third parties have access to covered data.

Prohibition on data access fees

The rule prohibits data providers from imposing fees on third parties for costs associated with covered data provision. Firms in the Aggregator Collection generally did not report paying fees to data providers for access to covered data per customer or per interface call, though a small number of annual or one-time payments were reported. Though these costs are currently limited, the provisions will ensure that the absence of fees under the baseline continues in the future, providing more certainty to third parties about their costs of accessing covered data. The CFPB does not have data to estimate the benefit to third parties of this prohibition on fees because of the uncertainty in how fees might have evolved under the baseline.

Reduced negotiation costs

As described in the *Benefits to data providers* part, based on data and comments provided by third parties, the CFPB estimates that negotiation costs will fall by 70 percent under the rule,

or an average savings of $24,000 per negotiated connection agreement. This will bring about substantial savings for third parties, particularly data aggregators. The reduction in negotiation costs may also allow additional third parties to enter into access agreements with data providers directly, potentially saving on expenses paid to aggregators under the baseline.

More frequent access to data

The rule prohibits covered data providers from unreasonably limiting the frequency of third party requests for covered data and from delaying responses to those requests. Based on responses to the Provider Collection and conversations with industry participants, the CFPB is aware that some large covered data providers that offer developer interfaces currently impose access caps. Third parties would benefit from the ability to access consumer data as often as is reasonably necessary to provide the requested service. One firm in the Aggregator Collection reported spending "significant resources" to manage its traffic in order to avoid access cap limits. Additionally, an aggregator in the Aggregator Collection reported spending resources to persuade large financial institutions to raise or eliminate access caps.

In addition to reducing costs associated with managing and limiting traffic, third party services may become more valuable to consumers when third parties can access consumer data more often.[187] As a result, the CFPB expects that third party revenue will increase from the removal of unreasonable access caps under the rule. The CFPB does not have data to quantify these benefits for third parties.

[187] For example, an app that warns consumers when the funds in their checking account fall below a predetermined threshold is generally more valuable to consumers when it can access data about their checking accounts more often.

Improved accuracy of data

The rule will require that data providers have policies and procedures reasonably designed to ensure the accuracy of data transmitted through their interfaces. In addition, the rule provides a consensus standards framework for several factors that third party small entity representatives reported as reducing accuracy, including data access reliability, inconsistencies in data field availability and formatting, and inaccuracies in screen scraped data.

The CFPB understands from the Aggregator Collection that access caps can prevent consumers from obtaining their most up-to-date data when a third party has surpassed its data limit. The removal of unreasonable access caps under the rule will reduce such issues. The rule will also require that a data provider make available the most recently updated covered data that it has in its control or possession at the time of a request, further ensuring that third parties will be more likely to have up-to-date data than under the baseline.

The transition away from screen scraping will lead to more consistency in the data fields that are available across all data providers and in data field formatting, and may reduce costs associated with ensuring that consumer data are accurate, particularly once consensus standards are established. One data aggregator reported more frequent inaccuracies for data accessed through screen scraping, as well as the need to allocate more resources to meet accuracy standards for screen scraped data. The CFPB understands that once compliant developer interfaces are established, third parties will need to transition away from screen scraping, which will reduce the costs associated with maintaining accuracy in screen scraped data.

Costs associated with maintaining accuracy in consumer data will not be eliminated altogether, as the rule will require that third parties ensure that covered data are accurately received from data providers, and accurately provided to other third parties, if applicable. The

CFPB expects that the increased accuracy of data received from data providers will simplify third party procedures for meeting data accuracy standards. Third party products and services are likely to become more valuable to consumers when data received from data providers is more accurate and reliable. The CFPB expects that this will increase third party revenue.

Improved service quality due to improved data access

As discussed in the *Benefits to third parties: Prohibition on data access fees* part, the rule will prevent data providers from charging fees to consumers or third parties for access to covered data, provide third party access to data from all covered data providers through compliant developer interfaces that meet reliability standards, eliminate unreasonable access caps, and improve the accuracy of received data. Furthermore, the rule clarifies that third parties are required to obtain authorization from consumers to access covered data, while data providers are permitted to confirm the scope of the third party's authorization. This will allow third parties to request the information that is reasonably necessary to deliver their product or service. These effects reduce third party costs of providing services to consumers and improve the quality of the services that they can provide. The CFPB expects that the ability to provide more valuable services to consumers at a lower cost would, over the short- to medium-term increase profits for existing third parties and lead to increased entry into the market for third parties' services.[188]

The rule is likely to enhance third party access to consumers' financial data, which could be used in third parties' credit underwriting decisions. Access to this data is likely to allow

[188] Third parties may experience an increase in investment under the proposed rule, in addition to a reduction in costs and improvement in service quality. Babina *et al.* (2023) study open banking polices adopted across 49 countries and find that fintechs, which include third party recipients of data, raised significantly more funding from venture capital following the implementation of open banking policies that require banks to share data with third parties. *See* Tania Babina *et al.*, *Customer Data Access and Fintech Entry: Early Evidence from Open Banking*, Stanford Univ. Graduate Sch. of Bus. Rsch. Paper (rev. Sept. 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4071214.

lenders to better differentiate between borrowers with different likelihoods of repayment and charge prices that are more aligned with potential borrowers' repayment risk, increasing underwriting profitability. As an example, the CFPB understands that access to consumer financial data enables some third party lenders to incorporate information about consumers' cash flow (*i.e.*, depository account inflows and outflows) into their underwriting models. Industry research has shown that cash flow is predictive of serious delinquency, and that models including cash flow can distinguish between the repayment risks of consumers with similar traditional credit profiles.[189] The CFPB expects that some third party lenders will be able to identify and reach more consumers with low repayment risk under the rule, and may therefore experience an increase in profits. The CFPB does not have data to quantify these benefits for third parties.

Reduced costs of establishing and maintaining screen scraping systems

The CFPB expects that third parties will cease screen scraping for covered data from covered data providers under the final rule. Based on the Aggregator Collection, the CFPB understands that maintaining screen scraping systems is more costly than maintaining developer interface connections. The reported ratio of staff hours spent on maintaining screen scraping data access to staff hours spent on maintaining interface data access ranged between 2.5 and 12. For aggregators that separately reported costs of maintaining data provider connections through both screen scraping and developer interfaces, the dollar cost of screen scraping ranged between $1.6 million and $7 million, or between $0.0005 and $0.0216 per access attempt; for developer

[189] One credit scoring company found that adding cash flow data to its traditional model improved predictiveness by 5 percent for consumers with thin or new credit profiles. Supporting this finding, FinRegLab studied six non-bank lenders in the current system and found the cash flow variables in their underwriting models were predictive of serious delinquency. *See* Can Arkali, *Icing on the Cake: How the FICO Score and alternative data work best together*, FICO Blog (June 2023), https://www.fico.com/blogs/icing-cake-how-fico-score-and-alternative-data-work-best-together; FinRegLab, *The Use of Cash-Flow Data in Underwriting Credit: Empirical Research Findings* (July 2019), https://finreglab.org/wp-content/uploads/2019/07/FRL_Research-Report_Final.pdf.

interfaces, the reported dollar cost was between $1.5 million and $1.6 million, or between $0.0001 and $0.0194 per access attempt. Each request made through a developer interface rather than through screen scraping leads to expected savings between $0.0004 and $0.0022. Cumulatively, the firms in the Aggregator Collection reported nearly 16 billion screen scraping attempts in 2022. Under the rule, these screen scraping attempts would instead be made through requests to developer interfaces, leading to at least $6.4 million to $35.9 million worth of annual savings for data aggregators, based only on information supplied by firms in the Aggregator Collection. Aggregators' savings may be passed on to data recipient third parties through lower prices for aggregator services. The CFPB expects that third parties' cost per access attempt will fall under the rule because screen scraping is more costly for third parties than accessing data through developer interfaces, and third parties will transition to only accessing covered financial data through interfaces.

Increased standardization

The CFPB expects that the cost of accessing consumer data will decrease not only through reductions in onboarding arrangement costs and screen scraping costs, but also because the rule incentivizes the industry to adopt consensus standards and requires standardized formats, including formats of data and communication protocol formats. The rule also clarifies which party is responsible for obtaining authorization from the consumer. The CFPB expects that increased standardization will be facilitated by one or more standard-setting bodies recognized by the CFPB, as outlined in the Industry Standard Setting rule.[190] One nondepository entity commenter expressed an expectation that this standardization will lead to increased market consolidation for data aggregator services. However, in order to deny covered data access to a

[190] 89 FR 49084 (June 11, 2024).

third party, data providers will need to meet the rule's requirements for reasonable denials. Data providers will also need to apply their covered data access denial standards in a consistent and non-discriminatory manner under the rule. This will limit the scope for data providers to partner with only a small number of dominant data aggregators if other data aggregators seek to access covered data and meet the requirements for covered data access. Additionally, the data provider will need to provide covered data in a standardized and machine-readable format and use standardized communication protocols to confirm with consumers the scope of a third party's authorization to the consumer's covered data. This increased standardization of data access will reduce the cost of providing data aggregator services under the rule, further reducing barriers to entry and increasing competition for data aggregator services. The CFPB further expects that increased standardization of data access may reduce the costs for third parties integrating with data providers and allow some third parties that provide services to consumers to bypass data aggregators. An increase in the share of third parties accessing data under access agreements with data providers would tend to reduce any degree of market power that data aggregators would enjoy under the baseline and will tend to reduce access prices for third parties. One small entity representative shared in the SBREFA process that aggregator costs represent its single largest budgetary line item, at approximately 10 percent of monthly expenditures. Data aggregators in the Aggregator Collection reported a wide range in fees charged to data recipient third parties depending on the recipient's size, minimum commitments, and access volume. Reported median annualized fees ranged between $2,000 and $6,000. Average annualized fees

ranged between $40,000 and $70,000, demonstrating that a small number of data recipients pay substantially more fees than average.[191]

The rule may make it comparatively less expensive for third parties to connect directly with data providers, rather than contracting with one or more data aggregators. Because a direct connection with a data provider is a substitute for aggregator services, a decrease in the cost of direct connections would likely decrease the price of aggregator services. However, because aggregators spread the costs of establishing data access agreements with each data provider across many authorized third parties, aggregators are likely to retain an advantage from scale in providing access. This advantage may decline over time with consensus standard development, which may reduce friction and cost associated with establishing and maintaining bespoke connections to each data provider. The CFPB does not have data to estimate the net benefits to data aggregators or data recipients due to increased standardization of data access.

4. Benefits to consumers

The rule will likely increase consumers' ability to access their covered data through third parties as desired. This increase may result in more third party products and services that consumers find useful in the marketplace. The use of credential-free data access will make this sharing possible without consumers revealing their credentials to third parties, reducing the potential harms that consumers may experience due to data breaches or similar incidents. Consumers will also have increased control over how third parties use their data, since third parties will no longer have indefinite authorization to use a consumer's covered data or to use it for reasons other than what is reasonably necessary to provide the product or service. The rule

[191] For example, responses in the Aggregator Collection suggested that a smaller number of data recipients may pay annualized fees totaling several million dollars.

will likely have important secondary benefits for consumers as well, for example through the development of new underwriting methods or increasing competition among data providers or third parties. Finally, the potential effects of the new financial data processing product or service definition are discussed below.

Right to third party data access

The rule will require data providers to facilitate consumer instructions to provide authorized third parties with covered data. As discussed in the section on *Benefits to third parties* in part VI.E.3, consumers' initial account connection attempts through authorized third parties experience high failure rates, and the rule benefits both consumers and third parties by guaranteeing authorized third parties the right to access covered data. Under the rule, data providers will be required to offer a developer interface with commercially reasonable performance, including a proper response rate in excess of 99.5 percent. This will benefit consumers by increasing the quality of third party products and services as well as the likelihood that consumers are able to use them at all. As discussed in the section on *Benefits to third parties* in part VI.E.3, the CFPB expects that third parties' costs of establishing connections with data providers will decline as a result of the rule, and this may benefit consumers to the extent that lower costs are passed through to them.

Further, guaranteed access to consumer authorized covered data will likely increase investment in third parties that request that data, providing consumers with more options in the marketplace and increasing competition.[192] As evidenced by the estimated 100 million

[192] For example, Babina *et al.* (2023) find that after other countries implemented open banking policies, venture capital investment in fintech companies increased significantly on average and the number of new entrants in the financial advice and mortgage markets increased. Tania Babina *et al.*, *Customer Data Access and Fintech Entry: Early Evidence from Open Banking,* Stanford Univ. Graduate Sch. of Bus. Rsch. Paper (rev. Jan. 22, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4071214.

consumers who have authorized third party data access discussed in the section on *Baseline* in part VI.D above, consumers have substantial demand for financial products and services offered by third parties, which may feature more convenient and automated means of gathering and using consumers' financial data relative to legacy financial service providers.[193] The CFPB expects that an expanded range of third party products and services will increase competition and innovation, offering important secondary benefits to consumers, including improved credit access and lower prices, discussed below.

Several bank commenters argued that the costs of the rule exceed the consumer benefits, and a bank and bank trade association argued that the costs of the developer interface exceed consumer benefits, especially for small data providers. The CFPB acknowledges, as discussed in the section on *Costs to data providers* in part VI.E.1 above, that data providers will incur costs associated with meeting developer interface requirements. The CFPB expects consumers to enjoy substantial benefits as a result of the ability to share consumer-authorized data with third parties as provided by the rule, such as the benefits described in the *effects of increased data sharing on innovation and competition* part. These benefits could reach over $1 billion annually even with relatively small increases in competition and account switching, as discussed in a more detailed analysis in this part. In addition, the non-coverage of depository institutions with assets below $850 million described in the rule alleviates the compliance costs for small depository institutions and substantially reduces the costs of the rule as a whole.

[193] As an example of how this can potentially increase access to credit for underserved populations, Howell *et al.* (2022) find that automation of underwriting processes for small business lending are associated with a higher share of loans being made to Black borrowers. Sabrina T. Howell *et al.*, *Lender Automation and Racial Disparities in Credit Access,* Nat'l Bureau of Econ. Rsch. Working Paper No. 29364 (Nov. 2022), https://www.nber.org/papers/w29364.

Commenters questioned the coverage of many data elements, but the CFPB expects that all data elements required by the rule provide consumer benefit. One bank argued that the costs of providing certain data elements, such as whether a borrower entered into an arbitration agreement as contained in account terms and conditions, is not outweighed by the benefits. Additionally, bank trade association, research institute, and credit union commenters stated that the consumer benefits of the requirement to provide terms and conditions do not outweigh the costs. The CFPB expects that as a general matter the provision of terms and conditions will benefit consumers by, for example, facilitating comparison shopping. Consumer knowledge of whether or not they are subject to an arbitration agreement will aid consumers in understanding their legal rights, which is a benefit in itself. The same commenters also argued against the inclusion of pending transactions stating that, for example, pending transactions may change in amount once settled. The CFPB expects that providing information about pending transactions can benefit consumers by, for example, alerting them about potential fraudulent charges, alerting them if they might be close to overdrafting, or allowing them to view their remaining credit limit on credit cards. These features have clear use cases in, for example, account monitoring and personal financial management. Based on the Aggregator Collection, tens of millions of inquiries were submitted for personal financial management and account monitoring in 2022. A bank trade association commented that providing data on rewards credit per transaction would be costly and that no evidence of benefits was provided. The CFPB expects that rewards programs information will help consumers comparison shop, and use any awards they accrue optimally. The CFPB does not have the data to perform a quantitative analysis, but the benefits from providing this information accrue to consumers over the long run, whereas the marginal cost of providing this information is limited and mostly incurred as a one-off, or fixed, expense. Accordingly, the

CFPB has determined that the potential consumer benefits can be significant in relation to costs, warranting the inclusion of this information. Some nondepository entity trade association, bank, and research institute commenters stated that the risks of requiring information to initiate payments outweighs the benefits to consumers. While the CFPB does not have data to perform a quantitative analysis, the CFPB has determined that requiring information to initiate payments supports highly beneficial consumer use cases such as account switching and making payments.

A credit union trade association commented that the CFPB should analyze whether data on non-covered products like mortgages is less beneficial to consumers than included data like credit card rewards, scheduled bill payments, and terms and conditions. The CFPB expects access to these types of covered data will benefit consumers. For example, information on scheduled bill payments has a clear personal financial planning benefit. The CFPB may pursue another rule in the future to cover other products, and has determined that the products and data covered by the current rule benefit consumers, as described in this part and in part IV.A.2.

One bank trade association argued that there is no consumer benefit to the requirement that data providers provide public quantitative performance metrics. The CFPB expects that this requirement will enable consumers and others to verify that data access is being provided consistently with the rule's requirements, and that consumers will benefit indirectly as the metrics will facilitate supervision and improve compliance with the rule. A commenter also stated that there is no consumer benefit to requiring three years of record retention instead of two. The CFPB has determined that a three-year record retention period provides sufficient information to conduct its exams and investigations, which, by enhancing compliance, benefit consumers.

One nondepository entity and two nondepository trade organizations argued that there is no benefit to covering digital wallets because transaction information is available more directly from bank account or credit card providers. As described in part IV.A.2, the CFPB expects that consumers will benefit from the rule's coverage of digital wallets because digital wallets may possess data from several depository institutions and account types, and because a digital wallet may offer a more convenient method for some consumers to provide third parties with consumer-authorized data. Further, a digital wallet may include information not available to the account-holding data provider, such as the time and location of the payment.

One community bank trade association commented that there is no evidence of significant demand among community bank customers for sharing data with third parties. The rule does not cover small depository institutions, and given the substantial demand for data sharing demonstrated in the Aggregator Collection and Provider Collection and the increasing availability of third party services, the CFPB finds it unlikely that there are institutions covered under the rule with little or no demand for data sharing among its customers.

Credential-free access—increased privacy, reduced data breach risks

Under the rule, data providers will be required to create an interface that can be used to share covered data with third parties without consumers' credentials being held by the third party. Many third parties currently use screen scraping techniques or credential-based APIs to access consumer information, which requires the consumer to provide the third party with their username and password for the data provider's website. This current practice may expose consumers to greater risk if a third party experiences a data breach. Such data breaches can be very costly for consumers. While the CFPB does not have data to estimate the resulting consumer benefits of credential-free access, the academic and practitioner literature indicates that

the associated benefits can be substantial.[194] Courts have approved large settlements in cases where data breaches affected financial service providers.[195] It is common for consumers to have their personal information compromised. For example, a 2019 Pew Research Center survey found that in the past 12 months, 28 percent of respondents reported having someone make fraudulent charges on their debit or credit card, take over a social media or email account without permission, or attempt to open a credit account in their name.[196] Under the rule, consumers would benefit from a reduced likelihood that third party data breaches would expose their account login information, since they would no longer have to give third parties their account credentials in order for the third party to access covered data. If the third party experienced a data breach it would be less likely to compromise the consumer's account since the breach would no longer potentially include the consumer's account access credentials. This in turn may reduce the risks of unauthorized transfers or other fraudulent account activity.

One nondepository entity commenter argued that since the market is already shifting towards APIs, the added benefit of the rule does not outweigh the costs. As discussed in this part,

---

[194] Albon *et al.* (2016) surveyed more than 6,000 consumers and found that in the previous year, 26 percent reported receiving a data breach notification. When asked about the costs that the data breach imposed on them, 68 percent of consumers whose data was breached estimated a nonzero financial loss, with a median value of $500. Lillian Ablon *et al.*, *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information,* RAND Corp. (2016), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1187/RAND_RR1187.pdf. A study of identity fraud by Javelin Strategy found that the average consumer who identified as a victim of identity fraud lost $1,551 and spent nine hours resolving the issue. Javelin Strategy, *Identity Fraud Losses Total $52 Billion in 2021, Impacting 42 Million U.S. Adults* (Mar. 29, 2022), https://javelinstrategy.com/press-release/identity-fraud-losses-total-52-billion-2021-impacting-42-million-us-adults. Consumers' liability for ATO fraud may be limited under Regulation E, but it is possible that not all consumers can or do successfully exercise their rights to limited liability.

[195] In 2019, a settlement for $190 million was approved in a data breach at Capital One that affected approximately 100 million consumers. Capital One, *Information on the Capital One cyber incident* (Apr. 22, 2022), https://www.capitalone.com/digital/facts2019/. A settlement of $425 million for consumers was reached in the 2017 Equifax data breach, which affected approximately 147 million consumers. Fed. Trade Comm'n, *Equifax Data Breach Settlement* (Dec. 2022), https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement.

[196] Brooke Auxier *et al.*, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Rsch. Ctr. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/how-americans-think-about-privacy-and-the-vulnerability-of-their-personal-data/.

the CFPB has determined that there are large potential benefits to consumers as a result of providers transitioning to credential-free access, and to the extent that data providers have already implemented interfaces meeting the requirements of the rule, the CFPB expects that these data providers will have lower costs of compliance. Further, the popularity of third party services and APIs highlights the need for safeguards to ensure consumer privacy. Another nondepository entity commenter stated that because some developer interfaces provide worse performance than legacy connection methods, shifting away from those legacy connection methods harms consumers. The CFPB has determined that the privacy and data security benefits of shifting to credential-free access outweigh any potential performance advantages of legacy methods under the baseline. Further, the CFPB expects the rule's performance standards for developer interfaces to improve the reliability of data access relative to screen scraping under the baseline. One third party and one consumer advocate commentator expressed concern that disallowing PII-based authentication methods could harm consumers without online accounts or credentials. The CFPB expects that all or nearly all consumers who wish to share consumer-authorized covered data with third parties either have an online account or the ability to create one. One data aggregator commentator expressed a concern that the transition away from screen scraping would harm consumers' ability to access accounts not covered by the rule, like mortgage and student loan accounts. However, the final rule does not affect screen scraping for accounts not covered by the final rule. Whether or not such screen scraping is permissible depends on other laws, such as the prohibition on unfair, deceptive, or abusive acts or practices, that form part of the baseline.

In addition, for a range of reasons, as this final rule takes operational effect, the CFPB expects some data providers and third parties to have compelling incentives to transition

voluntarily to credential-free interfaces for non-covered products that would have been accessed using credentials under the baseline. This would yield additional data security benefits to consumers.

Several commenters expressed concern about potential fraud risks that may occur even under credential-free authorization of third parties. One consumer advocate commenter and one credit union commenter said that if data are more readily available as a result of the rule, it could increase the risk of financial abuse and fraud, particularly for older consumers. Two consumer advocate commenters also expressed concern that the rule could increase availability of joint account information to domestic abusers. Two research entity commenters and a bank commenter stated that consumers might particularly be vulnerable to fraudulent pay-by-bank transactions. The CFPB acknowledges that a bad actor could potentially gain fraudulent access to consumer-permissioned data, but this risk exists under the baseline. The rule mitigates these risks through its authentication requirements and requirements for credential-free third party access. Practically, the CFPB expects that in order to connect a bank account to a new third party service, a bad actor would need access to the consumer's credentials for their covered account and potentially access to additional information or devices required for authorization, such as codes issued as part of two-factor authentication. These risks exist under the baseline, and the CFPB expects that any increased risks from greater use of consumer-permissioned data access are outweighed by the data security and privacy benefits of the rule.

Third party limitations on collection, use, and retention—ability to be forgotten, increased privacy, more control over use of own data

The rule will increase consumers' control over how their covered data are used by third parties. There is strong evidence that consumers value meaningful control over how their

personal information is used and thus consumers will benefit from the rule. In a 2015 survey, the Pew Research Center found that 93 percent of Americans said that it was very or somewhat important to be "in control of who can get information about you."[197] One consumer advocacy stakeholder stated that under the baseline, consumers may not understand how third parties share their data due to difficult-to-understand disclosures and may also not understand the rights they may have to limit how their data are shared. The Pew Research Center found in another study that 70 percent of Americans feel that their personal information is less secure than it was five years ago, 79 percent are very or somewhat concerned about how their personal information is being used by companies, and only 18 percent feel that they have a great deal of or some control over the data that companies collect about them.[198] Eighty-one percent feel that the potential risks of personal data collection by companies outweigh the benefits. This evidence suggests consumers have a strong desire for meaningful control over how their personal information is used and thus consumers will benefit substantially from the rule. The CFPB does not have sufficient data to provide a quantitative estimate of these benefits to consumers.

Effects of increased data sharing on innovation and competition

Increased availability of consumer-authorized data to third parties could have a number of other indirect—but potentially large—benefits for consumers. For example, as discussed in the section on *Costs to consumers* in part VI.E.2 above, while increased availability of data could result in lenders assessing some consumers as higher credit risk than they would be otherwise and charging them higher prices, it is also likely to result in lenders assessing some consumers as

[197] Pew Rsch. Ctr., *Americans Hold Strong Views About Privacy in Everyday Life* (May 19, 2015), https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/pi_15-05-20_privacysecurityattd00/.

[198] Brooke Auxier *et al.*, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Rsch. Ctr. (Nov. 2019), https://www.pewresearch.org/internet/2019/11/15/how-americans-think-about-privacy-and-the-vulnerability-of-their-personal-data/.

lower credit risk and charging them lower prices. It is possible that a consumer could be denied a loan that they would have been granted in the absence of the use of consumer-authorized data in underwriting. If the loan was not affordable for the consumer, then this denial could benefit the consumer in the long term.

Consumer-authorized data may be particularly useful for consumers who have a limited credit history or do not have a credit file with a nationwide consumer reporting company. Among consumers who do have credit scores, a study by FinRegLab found that cash-flow underwriting can help identify consumers who have low traditional credit scores but are actually a low credit risk for lenders.[199] It is possible that many consumers will experience increased access to credit or lower prices under the rule, to the extent that they are less able to share covered data with third parties under the baseline.[200] Even without the rule, the Aggregator Collection shows that in 2022, tens of millions of data requests were made through those data aggregators for consumer data to be used for underwriting purposes.[201]

The use of consumer-authorized covered data by third parties may also benefit consumers through increased availability and quality of payment services. The availability of consumer-authorized covered data may improve payment services by, for example, making it easier to sign

[199] FinRegLab, *The Use of Cash-Flow Data in Underwriting Credit* (July 2019), https://finreglab.org/wp-content/uploads/2019/07/FRL_Research-Report_Final.pdf.

[200] For example, using data from a German fintech lender, Nam (2024) finds that borrowers across the credit score distribution benefit on average when they choose to share data with the lender, with lower credit score borrowers experiencing a larger increase in acceptance rates and higher credit score borrowers experiencing a larger decrease in interest rates. *See* Rachel J. Nam, *Open Banking and Customer Data Sharing: Implications for Fintech Borrowers*, SAFE Working Paper No. 364 (Mar. 20, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4278803. One credit union trade association commenter stated that the CFPB did not consider data the effects of open banking in Europe. While the CFPB does not have primary data to analyze the effects of open banking on firms and consumers in other countries, it considered studies such as this one in its analysis.

[201] These requests include requests for information relating to existing accounts, like credit card limit increases, as well as the underwriting of new loans.

up for such services and allowing the service to verify a consumer's balance before initiating a payment to ensure that they are not overdrafting the consumer's account. In 2022, the Aggregator Collection shows nearly two billion requests for consumer data for facilitating payment services. Increased use of payment services is likely to benefit consumers.[202] Easier person-to-person payments may help consumers send or receive money from friends and family to avoid overdrafting their bank accounts or incurring fees through other forms of borrowing. In addition to providing benefits for person-to-person payments, consumer-authorized data are increasingly used to facilitate consumer-to-business "pay-by-bank" purchases, with lower fees relative to some alternatives, some of which may be passed through as benefits to consumers. One consumer advocate commenter expressed a concern that consumer-authorized covered data could be used to determine eligibility for government benefits, and that inaccuracy in the data could harm consumers. The CFPB expects that if widespread inaccuracies were a problem with an application using consumer-permissioned data to determine an eligibility for a program, it is unlikely that such an application would be used. A bank commenter raised a concern that covered data could be used to offer less competitive products by third parties. The CFPB acknowledges that third parties learn more about consumers though covered data, but notes that third parties' use of this data is limited by the rule to what is reasonably necessary to provide the consumer's requested service or product.

Increased availability of consumer -authorized covered data may also lower the costs for a consumer switching financial institutions in search of higher deposit rates, lower fees, better

[202] For example, Balyuk and Williams (2023) find that low-income consumers with increased exposure to a person-to-person payment platform are less likely to overdraft their bank accounts and more likely to borrow from family and friends using the platform if they have a low balance relative to their needs. *See* Tetyana Balyuk & Emily Williams, *Friends and Family Money: P2P Transfers and Financially Fragile Consumers* (Dec. 12, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3974749.

service, or lower rates on credit products. Recent research has found that digital banking technology affects the movement of deposits into and out of banks in response to market pressures.[203] The provisions may make it easier for a consumer to move to a new institution by easing the transfer of funds and account information from the old institution to the new institution.

Even marginal improvements in consumers' ability to shop for and transfer deposits could have large potential benefits for consumers, given the substantial size of the deposit market and the dispersion in prices across institutions. Consumers with sizeable savings may benefit most from accounts offering higher interest rates, while consumers with limited funds may benefit most from accounts with low or no fees. Recent studies suggest there is potential for substantial gains on both measures. On interest rates, researchers have documented high average savings interest rates available from large online banks, substantially above average savings interest rates.[204] On fees, the CFPB has found that although deposit account fees are trending lower since 2019, banks with over $1 billion in assets collectively earned $7.7 billion in revenue

[203] Koont, Santos and Zingales (2023) find that in response to Federal Funds rate changes, deposits flow out of banks with an online platform more quickly. Naz Koont *et al.*, *Destabilizing Digital Bank Walls* (Oct. 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4443273. Erel, Liebersohn, Yannelis, and Earnest (2024) found that primarily online banks saw larger inflows of interest-bearing deposits when Federal Funds rates increased. Isil Erel *et al.*, *Monetary Policy Transmission Through Online Banks*, Fisher Coll. of Bus. Working Paper No. 2023-03-015 & Charles A. Dice Ctr. Working Paper No. 2023-15 (June 3, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4459621.

[204] Erel, Liebersohn, Yannelis, and Earnest (2023) found that in April 2023, there were at least 15 large online banks offering an average savings interest rate of 2.17 percent, compared to 0.28 percent at other banks. Similarly, FDIC data from April 2023 show that, weighted by share of deposits, average savings interest rates were 0.39 percent. The authors also find that the online banks offer substantially higher rates for other products like certificates of deposit, individual retirement accounts, and money market deposit accounts. Isil Erel *et al.*, *Monetary Policy Transmission Through Online Banks*, Fisher Coll. of Bus. Working Paper No. 2023-03-015 & Charles A. Dice Ctr. Working Paper No. 2023-15 (May 26, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4459621; Fed. Deposit Ins. Corp., *FDIC National Rates and Rate Caps* (Apr. 17, 2023), https://www.fdic.gov/resources/bankers/national-rates/2023-04-17.html.

from overdraft and insufficient funds (NSF) fees in 2022.[205] This is despite the availability of at least 397 deposit account products with zero overdraft and NSF fees, with options available in every state.[206]

The rule will likely improve consumers' ability to switch providers. As a result, the rule will have two benefits. First, those consumers who switch may earn higher interest rates or pay lower fees. To estimate the potential size of this benefit, the CFPB assumes for this analysis that of the approximately $19 trillion[207] in domestic deposits at FDIC- and NCUA-insured institutions, a little under a third ($6 trillion) are interest-bearing deposits held by consumers, as opposed to accounts held by businesses or noninterest-bearing accounts.[208] If, due to the rule, even one percent of consumer deposits were shifted from lower earning deposit accounts to those

[205] Off. of Consumer Populations & Mkts., Consumer Fin. Prot. Bureau, *Overdraft/NSF revenue down nearly 50% versus pre-pandemic levels* (May 24, 2023), https://www.consumerfinance.gov/data-research/research-reports/data-spotlight-overdraft-nsf-revenue-in-q4-2022-down-nearly-50-versus-pre-pandemic-levels/full-report/.

[206] These accounts are certified as meeting the Bank On National Account Standards established by the Cities for Financial Empowerment Fund. See list of certified accounts at https://joinbankon.org/accounts/ (last visited Oct. 16, 2024), and current account standards, https://bankon.wpenginepowered.com/wp-content/uploads/2022/08/Bank-On-National-Account-Standards-2023-2024.pdf (last visited Oct. 16, 2024).

[207] Fed. Deposit Ins. Corp., *Insured Institution Performance*, 17(2) FDIC Quarterly (2023) https://www.fdic.gov/analysis/quarterly-banking-profile/qbp/2023mar/qbp.pdf, and Nat'l Credit Union Admin., *Quarterly Credit Union Data Summary* (2022 Q4), https://ncua.gov/files/publications/analysis/quarterly-data-summary-2022-Q4.pdf.

[208] Derived from several data sources, the assumption that slightly under one third of total deposits are interest-bearing deposits held by consumers is based on assuming slightly under half of all deposits are held by consumers, and about 70 percent of consumers' deposits are interest bearing. First, in the most recent available 2019 data from the Survey of Consumer Finances, households' mean savings in transaction accounts and certificates of deposit was $48,803; *see* Bd. of Governors of the Fed. Rsrv. Sys., *Survey of Consumer Finances (SCF)*, https://www.federalreserve.gov/econres/scfindex.htm (last updated Apr. 5, 2024). The 2020 Census estimates that there were 127 million U.S. households, and the product of these two numbers yields an estimate of $6.2 trillion in deposits held by consumers; *see* Thomas Gryn *et al.*, *Married Couple Households Made Up Most of Family Households*, America Counts: Stories, https://www.census.gov/library/stories/2023/05/family-households-still-the-majority.html. This is slightly under half of the $14 trillion in deposits based on Call Report data for 2019; Fed. Deposit Ins. Corp., *2019 Summary of Deposits Highlights*, 14(1) FDIC Quarterly (2020), https://www.fdic.gov/analysis/quarterly-banking-profile/fdic-quarterly/2020-vol14-1/fdic-v14n1-4q2019-article.pdf, Nat'l Credit Union Admin., *Quarterly Credit Union Data Summary* (2019 Q4), https://ncua.gov/files/publications/analysis/quarterly-data-summary-2019-Q4.pdf. The estimate for share of deposits that are interest bearing is derived from Figure A.3 in Erel, Liebersohn, Yannelis, and Earnest (2023). Isil Erel *et al.*, *Monetary Policy Transmission Through Online Banks*, Fisher Coll. of Bus. Working Paper No. 2023-03-015 & Charles A. Dice Ctr. Working Paper No. 2023-15 (May 26, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4459621.

with interest rates one percentage point (100 basis points) higher, consumers would earn an additional $600 million annually in interest. Similarly, if due to the rule, consumers were able to switch accounts and thereby avoid even one percent of the overdraft and NSF fees they currently pay, they would pay at least $77 million less in fees per year.[209]

The second potential way consumers could benefit is through improved prices and service even for consumers who do not switch providers, due to the rule's effects on competition. Increased competition from improved online banking services and open banking services under the baseline may have already contributed to consumers receiving higher interest rates on deposits and paying lower fees in recent years.[210] To estimate the scale of potential benefits from the provisions, if the rule further increases these competitive pressures such that average offered interest rates on deposits increase by even one basis point (0.01 percentage points), consumers would accrue an additional $600 million in annual benefits from interest even without moving their deposits. Similarly, if increased competitive pressures due to the rule caused banks to lower overdraft and NSF fees by one percent on average, consumers would benefit from at least $77 million in reduced fees annually.

---

[209] Survey evidence suggests that a small share of consumers value overdraft as a form of borrowing while a majority would prefer that the transactions were declined; *see* The Pew Ctr. on the States, *Overdraft America: Confusion an Concerns about Bank Practices* (May 2012), https://www.pewtrusts.org/~/media/legacy/uploadedfiles/pcs_assets/2012/sciboverdraft20america1pdf. In addition, the CFPB has found that some overdraft practices can be unfair, if they could not be reasonably anticipated; Consumer Fin. Prot. Bureau, *Unanticipated overdraft fee assessment practices*, Consumer Financial Protection Circular (Oct. 26, 2022), https://www.consumerfinance.gov/compliance/circulars/consumer-financial-protection-circular-2022-06-unanticipated-overdraft-fee-assessment-practices/. This analysis assumes that those consumers who prefer overdraft would stay with institutions offering these services, while those switching would prefer accounts without overdraft fees.

[210] Kang-Landsberg, Luck and Plosser (2023) find that the pass-through of the Federal Funds rate to deposit rates is increasing and nearing the levels seen in the early 2000s. Alena Kang-Landsberg *et al.*, *Deposit Betas: Up, Up, and Away?*, Liberty St. Econ. (Apr. 11, 2023), https://libertystreeteconomics.newyorkfed.org/2023/04/deposit-betas-up-up-and-away.

In addition to the effects in the deposit market, under the rule, a consumer's depository institution will no longer have a potential advantage in underwriting a loan based on the consumer's transaction data, which may increase competition and potentially lower interest rates on loan products for consumers. While these potential impacts are difficult to quantify, even marginal improvements in the interest rates or fees paid by consumers could have substantial benefits, given the size of consumer lending markets.

The provisions will also make it easier for consumers to access their data through personal financial management platforms. This increased ability to access and monitor information about their personal finances could benefit consumers.[211] The CFPB does not have data to quantify the resulting consumer benefit.

New financial data processing products or services definition

The CFPB expects that activities covered by the new financial data processing products or services definition are already within the scope of the CFPA's definition of financial product or service. As a result, the CFPB does not expect the new definition to have benefits to consumers. However, to the extent that there are firms offering products or services that are within the new definition but outside of the financial product or service definition, the new definition would benefit consumers by increasing protections against unfair, deceptive, or abusive acts or practices. The CFPB does not have data to quantify these potential benefits. The CFPB requested comment on whether any firms offer products or services that would be covered

[211] Carlin, Olafsson, and Pagel (2023) find that increased access to a personal financial management platform substantially lowers overdraft fees. Bruce Carlin *et al.*, *Mobile Apps and Financial Decision-Making*, 27 Rev. Fin. 977 (2023), https://academic.oup.com/rof/article/27/3/977/6619575. The evidence on this subject is mixed, however, as Medina (2021) finds that reminders to consumers to make credit card payments in a personal financial management platform increased the probability that consumers incurred overdraft fees and slightly increased overall net fees paid by consumers, since consumers were more likely to overdraft their bank account to pay their credit card bill. Paolina C Medina, *Side Effects of Nudging: Evidence from a Randomized Intervention in the Credit Card Market*, 34 Rev. Fin. Stud. 2580 (2021), https://academic.oup.com/rfs/article/34/5/2580/5903746.

by the new definition but fall outside the definition of financial product or service, and if so, what potential benefits to consumers could result from the new definition but did not receive any such comments.

5. Alternatives considered

The CFPB considered the impacts of several alternatives to the rule. These include alternatives that would allow secondary use of data by third parties in certain circumstances (*i.e.*, through an opt-in mechanism allowing the consumer to consent to specific uses, while retaining a prohibition on certain high-risk secondary uses) or allow retention and use of de-identified data as an exception to the general limitation standard that otherwise limits retention.[212] The CFPB considered covering Electronic Benefit Transfer accounts in the rule. The CFPB also considered alternatives specific to small entities, such as exemptions or longer compliance timelines, which are discussed in part VII.B.

Rather than prohibiting secondary uses, the CFPB considered allowing some secondary uses through an opt-in mechanism while prohibiting certain high-risk secondary uses. Relative to the proposal, this alternative would generally benefit third parties by allowing additional uses of data and potentially impose costs on consumers by reducing their privacy and their control of how their data are used. If these secondary uses lead to new beneficial products and services offered by third parties, this alternative could benefit consumers relative to the proposal. If, however, the additional secondary uses are detrimental to consumers despite the consumer's opt-in consent, allowing such uses could harm consumers relative to the baseline. The CFPB requested comment on whether any secondary uses should be allowed through an opt-in

[212] Some additional alternatives are considered and discussed in part IV. For example, alternatives to the prohibition on fees for establishing and maintaining interfaces and for accessing data through interfaces are discussed in part IV.C.2.

mechanism. The CFPB also requested comment on how potentially harmful secondary uses could be defined and prohibited under this alternative.

Comments on whether any secondary uses should be allowed through an opt-in mechanism and on how potentially harmful secondary uses could be defined and prohibited are discussed in parts IV.D.4, VI.E.1, and VI.E.2. In general, commenters' arguments about the benefits, costs, and impacts of allowing some secondary uses were in line with the CFPB's analysis of the benefits, costs, and impacts of this alternative, with data provider commenters generally opposed to allowing secondary uses, third party commenters generally in favor of allowing some secondary uses, and with varied support for this alternative from consumer advocate and research organization commenters. For the reasons discussed in parts IV.D.4, VI.E.1, VI.E.2, VI.E.3, and VI.E.4, the CFPB has determined that the rule as finalized better achieves the intended outcome of section 1033 of the CFPA than this alternative.

The CFPB also considered an exception to the general limitation standard for retention and use of de-identified data. Relative to the proposal, this alternative would generally benefit third parties by allowing the continued retention and use of de-identified consumer data after the general limitation standard would normally require the deletion of identified data. For example, de-identified data could potentially be used for product development, which would benefit third parties. These uses could also potentially benefit consumers through improved or new products. However, if the risk of reidentification remains for the consumers in de-identified data, the retention of such data creates a potential cost to consumers in privacy and fraud risks in the case of a data breach or misuse of data. In the proposal, the CFPB requested comment on whether there should be an exception to the general limitation standard for de-identified data, and if so, how de-identification should be defined to limit risks to consumers.

Comments on whether there should be an exception to the general limitation standard for de-identified data, and if so, how de-identification should be defined are discussed in parts IV.D.4, VI.E.1, and VI.E.2. In general, commenters' arguments about the benefits, costs, and impacts of an exception for de-identified data were in line with the CFPB's analysis of the benefits, costs, and impacts of this alternative, with data provider commenters generally opposed to an exception, third party commenters and research organization commenters generally in favor of an exception, and with varied support for this alternative from consumer advocate commenters. For the reasons discussed in parts IV.D.4, VI.E.1, VI.E.2, VI.E.3, and VI.E.4, the CFPB has determined that the rule as finalized better achieves the intended outcome of section 1033 of the CFPA than this alternative.

Finally, the CFPB considered including EBT accounts as covered accounts under the rule. Commenters stated that the impact analyses in the proposal did not consider the impact on EBT accountholders of not including EBT accounts in the rule. The CFPB considered the impacts of covering EBT accounts in the proposal, but found that several factors weighed against covering EBT accounts at this time. The CFPB acknowledges that many consumers use EBT accounts, and may not have reliable, convenient access to their account data provided by data providers. One nondepository entity commenter that provides third party data access to EBT accounts provided data on the prevalence and reliability of data sharing under their existing account connections. These data show that, under the baseline, rates of successfully accessing EBT data via existing third party connection methods range from 92 to 99 percent across EBT technology providers. Under the alternative in which such accounts were covered, consumers with EBT accounts would likely benefit from improved access through consumer interfaces, and improved third party access through developer interfaces. This improved access would benefit

consumers by making it easier to monitor their account balances and transactions. However, improved data access for EBT accounts would generally not provide the type of account switching and competition benefits quantified in the rule for deposit and credit card accounts, as EBT accounts are generally provided by government agencies, rather than through competing private firms. Based on these considerations and those described in part IV.A.3, the CFPB declines to expand coverage to EBT accounts at this time.

F. Potential Impacts on Insured Depository Institutions and Insured Credit Unions With $10 Billion or Less in Total Assets, as Described in Section 1026

Under the final rule, depository institutions (including credit unions, and including both federally insured and non-federally insured institutions) that satisfy the SBA definition of a small entity will not be required to maintain a consumer interface or developer interface. This is a change from the proposal. The final rule will require depository institutions with $10 billion or less in total assets (community banks and credit unions) but that do not satisfy the SBA definition of a small entity to maintain a consumer interface and a developer interface through which they receive requests for covered data and make that data available in an electronic form usable by consumers and authorized third parties. Compared to larger data providers, these institutions likely are more reliant on core banking providers and other service providers to comply, have fewer consumers and thus reduced efficiencies of scale, and may be less likely to act as data recipients in addition to being data providers. Compared to nondepository data providers of all sizes, these institutions may have more legacy systems that may be costly to modify to come into compliance with the proposal.

As discussed in part VI.E.1, the CFPB expects that most depositories of this size will contract with a vendor for their interfaces for consumers and third parties. To examine the types

of vendors used by covered institutions with $10 billion or less in total assets, the CFPB uses a data field in the NCUA Profile data which asks credit unions to indicate "the name of the primary share and loan information processing vendor."[213] While the vendor that provides core banking services to a credit union is not always the same vendor that provides digital banking services to the credit union, the CFPB expects that in many cases the same vendor provides both services. Based on the reported information for credit unions with between $850 million and $10 billion in assets, the CFPB estimates that at least 83 percent of such covered credit unions already use a vendor that offers interfaces for third parties. To measure the size of vendors used, the CFPB estimates that 97 percent of credit unions with between $850 million and $10 billion in assets use a vendor with at least 100 credit union clients, and 99 percent of such credit unions use a vendor with at least 50 credit union clients. The CFPB expects that many of these vendors would likely offer interfaces for third parties by the compliance date applicable for community banks and credit unions. However, the 1 percent of credit unions using smaller vendors are more likely to need to either switch vendors or build a developer interface in house. This could lead to higher costs, as the costs of switching to a new vendor may be larger as a proportion of total assets or revenues for smaller depositories relative to larger depositories.

The CFPB does not have data on the vendors used by community banks, but expects that they may have a similar distribution of vendors as the comparably sized credit unions, and thus will face comparable costs to establish a developer interface.

The CFPB requested comment on its analysis in the proposal of the potential impact on depository institutions and credit unions with $10 billion or less in total assets. The CFPB did not

[213] A "share" denotes a deposit account held by a credit union, and thus will include the Regulation E covered accounts under the proposal.

receive comments specifically on its analysis of potential impacts on insured depositories and insured credit unions with less than $10 billion in assets, but comments that addressed impacts on small depositories, credit unions, and community banks are discussed in parts VI.E.1, VI.E.3, and VII.B.

G. Potential Impacts on Consumers in Rural Areas, as Described in Section 1026

Relative to the proposal, the CFPB expects that the change in coverage for depositories that satisfy the SBA definition of small entities and the extended compliance timelines will substantially reduce the impacts of the rule on consumers in rural areas.

Under the baseline, smaller banks hold a larger share of deposits in rural areas. For example, analysis by the Federal Reserve Board in 2017 found that the market share of community banks (defined as assets of less than $10 billion) in rural areas is nearly 80 percent on average, compared with nearly 40 percent in urban areas.[214]

Rural consumers are substantially less likely to use online banking than those who live in urban areas, defined to include all MSAs. For example, Benson *et al.* (2020) find that 56 percent of consumers in rural areas use online banking compared to 75 percent in large MSAs.[215] This may generally mean that rural consumers could experience less of both the costs and the benefits of the rule. Some of the difference in online banking use may be explained by differences in access to high-speed internet, since as of 2018 consumers in rural areas were 20.8 percentage points less likely to have the option of subscribing to high-speed internet.[216] Given that rural

[214] Bd. of Governors of the Fed. Rsrv. Sys., *Trends in Urban and Rural Community Banks* (Oct. 4, 2018), https://www.federalreserve.gov/newsevents/speech/quarles20181004a.htm.

[215] David Benson *et al.*, *How do Rural and Urban Retail Banking Customers Differ?*, FEDS Notes (June 12, 2020), https://www.federalreserve.gov/econres/notes/feds-notes/how-do-rural-and-urban-retail-banking-customers-differ-20200612.html.

[216] Fed. Commc'ns Comm'n, *2020 Broadband Deployment Report* (released Apr. 24, 2020), https://docs.fcc.gov/public/attachments/FCC-20-50A1.pdf.

consumers are less likely to use online banking, they may also be less likely to use third party online services. The CFPB does not have comprehensive data on the geographic distribution of the use of third party products and services, though since rural consumers are less likely to have high-speed internet access, they may be less likely to use third party products and services. The 2021 FDIC National Survey of Unbanked and Underbanked Households found that 68.7 percent of consumers with bank accounts outside of MSAs had linked their bank account to a third party online payment service, compared with 72.3 percent in MSAs, showing that rural consumers are slightly less likely to use at least one type of third party product.[217]

The CFPB requested comment on its analysis in the proposal of potential impacts on consumers in rural areas. One consumer advocate commenter noted that consumers in rural areas may be more likely to live in banking deserts and thus more reliant on online financial services like those offered by third parties. The CFPB expects that the final rule will increase the availability of such online services for consumers in rural areas who bank at covered data providers. The rule also implements additional protections for consumers using third party services. For consumers who bank at data providers not covered by the rule, the CFPB expects that data access will generally continue to improve as it has under the baseline, through voluntary adoption of new methods of third party data access.

More general comments on impacts on consumers, including consumers who bank at community banks or credit unions, are discussed in parts VI.E.2 and VI.E.4.

[217] Fed. Deposit Ins. Corp., *2021 National Survey of Unbanked and Underbanked Households*, https://www.fdic.gov/analysis/household-survey/index.html (last updated July 24, 2023).

VII. Regulatory Flexibility Act Analysis

The Regulatory Flexibility Act (RFA)[218] generally requires an agency to conduct an IRFA and a FRFA of any rule subject to notice-and-comment requirements. These analyses must "describe the impact of the proposed rule on small entities."[219] An IRFA or FRFA is not required if the agency certifies that the rule will not have a significant economic impact on a substantial number of small entities.[220] The CFPB also is subject to certain additional procedures under the RFA involving the convening of a panel to consult with small business representatives prior to proposing a rule for which an IRFA is required.[221] The CFPB did not certify that the proposed rule would not have a significant economic impact on a substantial number of small entities within the meaning of the RFA. Accordingly, the CFPB convened and chaired a Small Business Review Panel under SBREFA to consider the impact of the proposed rule on small entities that would be subject to that rule and to obtain feedback from representatives of such small entities. The Small Business Review Panel for the proposal is discussed in part VII.A. The CFPB is also publishing a FRFA. Among other things, the FRFA estimates the number of small entities that will be subject to the rule and describes the impact of that rule on those entities. The FRFA for this rule is set forth in part VII.B.

[218] 5 U.S.C. 601 *et seq*.

[219] 5 U.S.C. 603(a). For purposes of assessing the impacts of the proposed rule on small entities, the term "small entities" is defined in the RFA to include small businesses, small not-for-profit organizations, and small government jurisdictions. 5 U.S.C. 601(6). A "small business" is determined by application of SBA regulations and reference to the NAICS classifications and size standards. 5 U.S.C. 601(3). A "small organization" is any "not-for-profit enterprise which is independently owned and operated and is not dominant in its field." 5 U.S.C. 601(4). A "small governmental jurisdiction" is the government of a city, county, town, township, village, school district, or special district with a population of less than 50,000. 5 U.S.C. 601(5).

[220] 5 U.S.C. 605(b).

[221] 5 U.S.C. 609.

A. Small Business Review Panel

Under section 609(b) of the RFA, as amended by SBREFA and the CFPA, the CFPB must seek, prior to conducting the IRFA, information from representatives of small entities that may potentially be affected by its proposed rules to assess the potential impacts of that rule on such small entities.

The CFPB complied with this requirement. Details on the SBREFA Panel and SBREFA Panel Report for the proposal are described in part II.A.

B. Final Regulatory Flexibility Analysis

1. Statement of the need for, and objectives of, the rule

In section 1033 of the CFPA, Congress authorized and directed the CFPB to adopt regulations governing consumers' data access rights. The CFPB is issuing this rule primarily to implement CFPA section 1033 with respect to certain covered persons under the CFPA, although the CFPB is also relying on other CFPA authorities for specific aspects of the rule. This rule aims to (1) expand consumers' access to their financial data across a wide range of financial institutions, (2) ensure privacy and data security for consumers by limiting the collection, use, and retention of data that is not needed to provide the consumer's requested service, and (3) push for greater efficiency and reliability of data access across the industry to reduce industry costs, facilitate competition, and support the development of beneficial products and services. The CFPB is issuing this rule pursuant to its authority under the CFPA. The specific CFPA provisions relied upon are discussed in part III. See part VI.A for additional discussion of the objectives of the rule.

2. Significant issues raised by public comments in response to the IRFA, a statement of the assessment of the agency of such issues, and a statement of any changes made in the proposed rule as a result of such comments

Trade associations representing small depository institutions requested that the CFPB provide flexibilities or less costly alternatives for small entities. Comments from such organizations and from small depository data providers themselves stated that the CFPB conducted an incomplete analysis of the disproportionate costs of the proposal on smaller entities. Data provider commenters also stated that the costs from the rule would work against small and mid-sized banks, since larger banks already have the functionality and are able to take advantage of scale. A data provider industry association commenter stated that the CFPB did not take into account the feedback received through the SBREFA process, and that the CFPB should consider how increased competition from fintechs will impact credit unions. A credit union industry association commented that the RFA analysis in the proposal was flawed in how it approached credit union's costs as data providers because it did not take into account the cumulative regulatory impact of different rulemakings on credit unions.

The CFPB has determined that it is appropriate to not finalize the proposed coverage of the rule, such that small entity depositories are not covered as data providers. As a result, under the final rule, small entity depositories will not face any costs to maintain a consumer or developer interface due to the rule.

The CFPB expects that this change will address the concerns of small entity commenters, but notes that the impact analyses in the proposal did account for feedback received through the SBREFA process and did provide a complete analysis of the differential costs to small entities. Based on its analysis and the feedback received during that process, the proposal reduced the

number and complexity of required data fields in the proposal relative to the SBREFA Outline, and established longer compliance timelines for small entities. These provisions of the proposal were an acknowledgement of the reliance of small depository data providers on service providers to comply with the rule and the scale advantages of large data providers. Regarding increased competition from fintechs, the proposal acknowledged that there would likely be increased competition for covered accounts, due to easier account switching and enhanced services offered by third parties under the rule. The trend of greater competition from third parties is likely heightened under the rule, although it is present under the baseline as well; this trend also stands to benefit small data providers with competitive account offerings. The CFPB expects that many small entity data providers will adopt developer interfaces voluntarily due to competitive pressures, as they have done prior to the rule, but the change in coverage will allow small data providers to forgo or delay the deployment of a developer interface if it is especially costly for them based on the characteristics of their institution. Regarding the comment asserting there is a cumulative impact of different rulemakings on credit unions, small entities that are credit unions are not data providers under the final rule.

3. *Response of the agency to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration in response to the proposed rule, and a detailed statement of any change made to the proposed rule in the final rule as a result of the comments*

The Chief Counsel for Advocacy of the Small Business Association (Advocacy) provided comments on several aspects of the proposal. Advocacy stated that the exemptions in the proposal were too narrow, and that the CFPB should consider exemptions for small third parties in addition to any exemptions for data providers. Advocacy commented that implementation timelines should be longer. Advocacy also commented that the CFPB did not discuss the

possibility that firms may reduce their offerings to customers rather than comply, and that the CFPB should analyze the impact if small entities decide to exit rather than comply with the rule. Advocacy stated that the CFPB should consider State laws that have similar requirements, and evaluate if the rule is necessary or creates additional burden. Advocacy commented that the CFPB should clarify the role of industry standards and the responsibility or liability for data security issues or misuse of data. Advocacy commented that small entities should be permitted to charge fees for making covered data available, and that the CFPB should reduce the definition of covered data for transaction information to 12 months, rather than the "safe harbor" of 24 months in the proposal.

In the final rule, the CFPB has revised the proposed coverage such that small entity depositories are not covered as data providers. With regards to small depository data providers, this change also addresses Advocacy's comments about the possibility that firms may reduce their service offerings or decide to exit the market in response to the rule.

The CFPB considered exemptions for small nondepository data providers, but generally understands that these firms do not have the technological complexities that make complying with the data provider requirements as burdensome as for depositories. Rather than exempt some small nondepository data providers, the CFPB has instead extended the compliance deadlines for such entities from one year in the proposal to approximately 2.5 years in the final rule. The CFPB expects this change to substantially mitigate the burden of compliance for small nondepository data providers.

The CFPB considered exemptions for small third parties in the proposal, but remains concerned that allowing third parties to access covered data via the rule without requiring the data security, data privacy, and secondary use restrictions in the rule would significantly reduce

the benefits to consumers and would create risks for data providers—including small entity data providers. In addition, unlike covered data providers, small entities that are potential third parties have a choice over whether to access covered data, and can choose not to access such data if they find that complying with the rule's authorization requirements and secondary use restrictions are too costly. As described in part VI.E, the CFPB expects that compliance costs for third parties will be less burdensome than costs for data providers and that benefits to third parties will outweigh the costs. As a result, the CFPB does not expect the rule's requirements on third parties to deter the development of beneficial third party products and services.

Regarding the consideration of State laws that have similar requirements, the CFPB considered such laws, as described in part VI.D. These primarily include State-level data privacy and data security laws, which are closest in effect to some of the rule's requirements on third parties. The CFPB expects the rule's requirements on third parties to be complementary to these State laws, and necessary to impose on all third parties, regardless of where they operate or where their consumers are located, to limit data privacy and security risks to consumers. In addition, State laws generally do not require data providers to provide consumers with access to their financial data, which is the core objective of CFPA section 1033 and this rule.

Regarding the clarity of industry standards, as discussed in part II.C, the CFPB published the Industry Standard-Setting Final Rule in June 2024 to try to provide clarity on industry standards sooner and to ease compliance burden for industry participants, including small entities.

The potential costs related to liability or fraud for data providers are discussed in part VI.E.1. As discussed in that part, the CFPB expects that the majority of data providers will see a net decrease in fraud risks and reputational risks relative to the baseline of current market

practices, in which screen scraping is widespread and there are no restrictions on data collection, retention, and use by third parties. Small depository entities are not covered as data providers under the final rule, and the CFPB generally expects that liability and fraud risks will be reduced for the majority of small nondepository data providers, based on the evidence discussed in part VI.E.1.

Regarding permitting small data providers to charge fees for access, the CFPB has declined to permit such fees for the reasons discussed in parts IV.C.2 and VI.E.1. The CFPB has also declined to change the definition of covered data for transaction information held by small entity data providers, for the reasons discussed in part IV.B.3. The CFPB has instead addressed burden on small entities through revisions to coverage, compliance timelines, and other revisions relative to the proposal as discussed in this part.

4. Description of and an estimate of the number of small entities to which the rule will apply or an explanation of why no such estimate is available

The small entities affected by the rule will be those that meet the definitions of data provider, third party, or data aggregator. Data providers include depository institutions and nondepository institutions, although, as discussed above, small depository institutions are not covered. The new financial data processing product or service definition will apply to third parties, data aggregators, or others that provide financial data processing products or services for consumer purposes.

Nondepository financial institutions and entities outside of the financial industry may also be affected, though it is important to note that entities within these industries will only be subject to the rule if they meet the definitions of data provider, third party, or data aggregator. Examples of potentially affected small third parties include entities using consumer-authorized

data to underwrite loans, offer budgeting or personal financial management services, or facilitate payments.

For the purposes of assessing the impacts of the rule on small entities, "small entities" are defined in the RFA to include small businesses, small nonprofit organizations, and small government jurisdictions. A "small business" is defined by the SBA's Office of Size Standards for all industries in the NAICS. The CFPB has identified several categories of small entities that may be subject to the proposals under consideration. These include depository institutions (such as commercial banks, savings associations, and credit unions), credit card issuing nondepositories, sales financing companies, consumer lending companies, real estate credit companies, firms that engage in financial transactions processing, reserve, and clearinghouse activities, firms that engage in other activities related to credit intermediation, investment banking and securities dealing companies, securities brokerage companies, and commodities contracts brokerage companies. Other potentially affected small entities include software publishers, firms that provide data processing and hosting services, firms that provide payroll services, firms that provide custom computer programming services, and credit bureaus. According to the SBA's Office of Size Standards, depository institutions are small if they have less than $850 million in assets. Nondepository firms that may be subject to the rule have a maximum size of $47 million in receipts, but the threshold is lower for some NAICS categories.[222] Table 1 shows the number of small businesses within NAICS categories that may be subject to the rule based on December 2023 NCUA and FFIEC Call Report data and 2017

[222] SBA regularly updates its size thresholds to account for inflation and other factors. The SBA Size Standards described here reflect the thresholds in effect at the publication date of this final rule. The 2017 Economic Census data are the most recently available data with entity counts by annual revenue. *See* Small Bus. Admin., *SBA Size Standards* (effective Mar. 17, 2023), https://www.sba.gov/sites/sbagov/files/2023-06/Table%20of%20Size%20Standards_Effective%20March%2017%2C%202023%20%282%29.pdf.

Economic Census data from the U.S. Census Bureau. Entity counts are not provided for the specific revenue amounts that the SBA uses to define small entities and are instead usually provided at multiples of five or ten million dollars. Table 1 includes the closest upper and lower estimates for each revenue limit (*e.g.*, a NAICS category with a maximum size of $47 million in receipts has both the count of entities with less than $50 million in revenue and the count of entities with less than $40 million in revenue). Not all small entities within each included NAICS category will be subject to the rule.

Table 1: Number of small businesses within NAICS industry codes that may be subject to the rule

	Number of Entities	**Percent of Entities**
A. Small Depository Firms		
Commercial Banking (522110), Savings Institutions (522120), and Credit Card Issuing (522210)	4,587	
< $850M (Assets)	3,422	74.6%
Credit Unions (522130)	4,702	
< $850M (Assets)	4,202	89.4%
B. Small Nondepository Firms		
Software Publishers (511210)	10,014	
< $40M (Revenue)	9,395	93.8%
< $50M (Revenue)	9,461	94.5%
Data Processing, Hosting, and Related Services (518210)	10,860	
< $40M (Revenue)	9,930	91.4%
Sales Financing (522220)	2,367	
< $40M (Revenue)	2,112	89.2%
< $50M (Revenue)	2,124	89.7%
Consumer Lending (522291)	3,037	
< $40M (Revenue)	2,905	95.7%
< $50M (Revenue)	2,915	96.0%
Real Estate Credit (522292)	3,289	
< $40M (Revenue)	2,872	87.3%
< $50M (Revenue)	2,904	88.3%
Financial Transactions Processing, Reserve, and Clearinghouse Activities (522320)	3,068	

	Number of Entities	Percent of Entities
< $40M (Revenue)	2,916	95.0%
< $50M (Revenue)	2,928	95.4%
Other Activities Related to Credit Intermediation (522390)	3,772	
< $25M (Revenue)	3,610	95.7%
< $30M (Revenue)	3,621	96.0%
Investment Banking and Securities Dealing (523110)	2,394	
< $40M (Revenue)	2,214	92.5%
< $50M (Revenue)	2,227	93.0%
Securities Brokerage (523120)	6,919	
< $40M (Revenue)	6,703	96.9%
< $50M (Revenue)	6,717	97.1%
Commodities Contracts Brokerage (523140)	856	
< $40M (Revenue)	825	96.4%
< $50M (Revenue)	829	96.8%
Payroll Services (541214)	4,328	
< $35M (Revenue)	4,111	95.0%
< $40M (Revenue)	4,116	95.1%
Custom Computer Programming Services (541511)	62,205	
< $30M (Revenue)	60,959	98.0%
< $35M (Revenue)	61,088	98.2%
Credit Bureaus (561450)	307	
< $35M (Revenue)	279	90.9%
< $75M (Revenue)	283	92.2%

Table 2 provides the CFPB's estimate of the actual number of affected entities within the categories of depositories, nondepository data providers, and third parties, and the NAICS codes these entities may fall within. As described in part VII.B.6, with regard to the requirements of the rule applicable to data providers, the final rule does not cover depositories that are small entities based on SBA's definition. As a result, there will be no small entity depositories covered by the rule, in their capacity as data providers. If any of these entities operate as third parties, they will be covered and counted as third parties. The CFPB is not able to estimate with precision the number of small nondepository entities that will be subject to the rule, but expects that approximately 100 small nondepository institutions will be data providers under the rule. In

addition, based on data from the Provider Collection and Aggregator Collection, the CFPB estimates that between 6,800 and 9,500 small entities are third parties that access consumer-authorized data.

Table 2: Estimated number of affected entities and small entities by category

Category	NAICS	Small Entity Threshold	Est. Total Affected Entities	Est. Number of Small Entities
Depository institution data providers	522110, 522120, 522130, 522210	$850 million in assets	1,665	0
Nondepository financial institution data providers	511210, 522291, 522320	Varies, less than $47 million in annual receipts	120	100
Third parties	511210, 518210, 522110, 522120, 522130, 522210, 522220, 522291, 522292, 522320, 522390, 523110, 523120, 523140, 541214, 541511, 561450	Varies, less than $47 million in annual receipts, or less than $850 million in assets for depository third parties	7,000–10,000	6,800–9,500

5. *Projected reporting, recordkeeping, and other compliance requirements of the rule, including an estimate of the classes of small entities which will be subject to the requirement and the type of professional skills necessary for the preparation of the report or record*

The rule will impose new reporting, recordkeeping, and other compliance requirements on small entities subject to the rule, which excludes small depository data providers. These requirements generally differ for small entities in two classes: nondepository data providers and third parties. Part VI.E provides a detailed description of the requirements and estimated compliance costs that will be faced by affected small entities under the rule. These requirements will be imposed on an estimated 100 small nondepository data providers and between 6,800 and 9,500 small third parties, as shown in Table 2. The requirements and their costs are summarized in this section.

Requirements for nondepository data providers

The rule will require nondepository data providers to calculate and disclose the response rate for third party data access on a monthly basis. The CFPB estimates that data providers may face a $7,600 cost of developing and testing a system to regularly disclose this information on their websites. The CFPB expects these reports will generally be automated and will have minimal ongoing costs after the system is implemented.

The rule will require nondepository data providers to have policies and procedures to retain records to demonstrate compliance with certain other requirements of the rule. Data providers will also be required to have policies and procedures designed to ensure that the reason for the decision to decline a third party's request to access its developer interface is communicated to the third party. The CFPB expects that these recordkeeping requirements will likely be built into a data provider's developer interface and the cost methodology described in

part IV.E.1 includes these in the overall cost of establishing and maintaining a compliant developer interface. Incremental costs of these requirements are limited to developing and implementing reasonable policies and procedures, which the CFPB estimates will cost $23,500 to $51,200 per data provider.

The rule requires nondepository data providers to maintain a consumer interface that allows consumers to directly access their data. As discussed in part VI.E.1, the CFPB expects that data providers subject to this requirement generally already provide the required information under the baseline and estimates that the incremental costs of this requirement will be minimal.

The rule requires nondepository data providers to maintain a developer interface. As described in part VI.E.1, the CFPB expects that most nondepository data providers will develop and maintain their developer interfaces in-house. For small nondepository data providers that choose to build their developer interface in-house, the estimated upfront cost is $46,000. Estimated annual costs for in-house developer interfaces include technology costs of $20,000 as well as ongoing staffing costs of $48,000 to $95,000.

The rule requires data providers to have policies and procedures to ensure that data are accurately transferred to third parties. In the cost methodology described in part IV.E.1, the CFPB includes these costs in the estimate for establishing and maintaining a compliant developer interface.

Satisfying these requirements for data providers would generally involve professional skills related to software development, general and operational management, legal expertise, compliance, and customer support.

Requirements for third parties

Third parties are not subject to reporting requirements but will be required to retain records of consumer data access requests and actions taken in response to these requests, reasons for not making the data available, and data access denials under the rule. The CFPB understands that most third parties maintain similar records and costs will be limited to a one-time change to existing systems and small storage costs. The CFPB estimates a one-time cost of $10,100 for third parties to develop and implement appropriate policies and procedures, with minimal ongoing costs.

The rule requires third parties to establish and maintain systems that receive data access revocation requests, track duration-limited authorizations, delete data when required due to revoked or lapsed authorizations, and retain the relevant records. The CFPB estimates that the one-time cost to establish these systems will be between $22,800 and $94,900, with minimal ongoing costs.

The rule requires third parties to provide authorization disclosure and certification statements. The CFPB estimates that the one-time cost to third parties of establishing an automated system to provide these disclosures would be $94,000. However, the CFPB expects that small third parties will generally use another third party to provide these disclosures and this cost will not be incurred. If third parties currently provide disclosures, modifying the content to comply with the proposed rule is estimated to cost between $2,900 and $3,800.

Satisfying these requirements for data providers will generally involve professional skills related to software development, general and operational management, legal expertise, compliance, and customer support.

As discussed in part VI.E.1, the CFPB does not expect the new financial data processing products or services definition to impose costs on small entities.

6. *Description of steps the agency has taken to minimize the significant economic impact on small entities consistent with the stated objectives of applicable statutes, including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected*

In the proposal, the CFPB considered several alternatives to the proposal that would minimize economic impacts on small entities. These alternatives generally fell into four categories: (1) limiting coverage of small data providers, (2) permitting small data providers to charge fees for making covered data available, (3) exemptions from the proposed rule for small third parties, or (4) alternative compliance dates for small depository data providers.

In the final rule, small depositories are not covered data providers. While the CFPB considered more limited alternatives for excluding depository data providers from coverage in the proposal, comments from the SBA Office of Advocacy and data provider commenters nearly universally favored coverage definitions that would reduce burden for a larger number of small depository data providers. The CFPB has revised the coverage of depository data providers in the final rule to reduce the burden on small depository data providers, thereby addressing these comments.

The CFPB considered not covering small nondepository data providers. However, as discussed in part VII.B.3, the CFPB has determined that compliance burdens are likely to be lower for these small entities as compared to small depositories, and that extended compliance

timelines would better address burden on small nondepositories while still accomplishing the goals of the rulemaking.

The CFPB also considered the alternative of permitting small data providers to charge fees for making covered data available through developer interfaces. Given the change in coverage in the final rule, this alternative would only affect small nondepository data providers. The CFPB has determined that a data provider charging such fees would be inconsistent with the data provider's statutory obligation under CFPA section 1033 to make covered data available to consumers and to their authorized third party representatives. Further, consumers at covered small data providers could be harmed through reduced access to third parties' products and services if the CFPB were to permit only small data providers to charge fees.

The CFPB also considered exemptions as a means to reduce burden for small entity third parties. Based on data from the Aggregator Collection, the CFPB estimates that there are approximately 6,800 to 9,500 third parties with fewer than 100,000 connected accounts, many of which may be small entities. However, exempting third parties from certain conditions of access under the rule, such as the requirements on collection, use, and retention, would likely create risks of harm for consumers on data security and privacy grounds, provide unfair competitive advantages for exempt versus non-exempt third parties, and increase the risks of losses from data security incidents for consumers and data providers.

Finally, the CFPB considered alternative compliance dates for small entities to reduce burden. The proposed rule had a compliance date of approximately four years after the final rule is published in the *Federal Register* for depository data providers with less than $850 million in assets. In the final rule, small depositories are not covered as data providers. For small nondepository data providers, the CFPB has extended the compliance date from approximately

one year after the final rule is published in the *Federal Register* to approximately 2.5 years after publication. The CFPB expects this will substantially reduce compliance burden on small nondepository data providers. Regarding potential burden for small third parties, the CFPB has also extended the earliest compliance dates that apply to the largest data providers from six months to approximately 1.5 years and published the Industry Standard-Setting Final Rule in June 2024 to encourage the establishment of consensus standards in the near future. The CFPB expects these changes to effectively increase the amount of time small third parties have to come into compliance with the rule, reducing their compliance burden.

7. Description of the steps the agency has taken to minimize any additional cost of credit for small entities

The CFPB expects that the rule may have some limited impact on the cost or availability of credit for small entities but does not expect that the impact will be substantial. The CFPB expects there are several ways the rule could potentially impact the cost or availability of credit to small entities. First, the provisions of the rule could impact the availability of credit to small entities if small businesses are using loans from lenders (either data providers or third parties) affected by the provisions and the provisions lead to a contraction of the offered services. Second, the rule could potentially increase the cost of credit for small businesses if the costs of implementing the rule are passed through in the form of higher prices on loans from lenders. Third, for small business owners that use consumer-authorized data to qualify for or access credit, the provisions could potentially increase credit availability or lower costs for small entities by facilitating increased data access.[223] Small entity representatives did not provide

[223] As an example, Howell *et al.* found that more automated fintech lenders facilitated a higher share of Paycheck Protection Program loans to small, Black-owned firms relative to traditional lenders. Sabrina T. Howell *et al.*, *Lender Automation and Racial Disparities in Credit Access*, 79 J. Fin. 1457-1512 (202), https://doi.org/10.1111/jofi.13303.

feedback on this topic during the SBREFA process.[224] The CFPB did not have data to quantify these potential impacts in the proposal.

The CFPB requested comment on its analysis of the proposal's impact on the cost of credit for small entities, and requested data or evidence on these potential impacts. One consumer advocate commenter stated that open banking and access to online providers give small businesses access to new services, but cited a study finding that surveyed small businesses had lower satisfaction with online lenders than with small banks.[225] The CFPB expects that the rule will generally improve small businesses' ability to use online financial services, increasing their options for credit. The CFPB also expects that the final rule's coverage and extended implementation periods will reduce compliance burden on small depositories relative to the proposal, mitigating negative effects on credit access.

VIII. Paperwork Reduction Act

Under the Paperwork Reduction Act of 1995 (PRA),[226] Federal agencies are generally required to seek, prior to implementation, approval from OMB for information collection requirements. Under the PRA, the CFPB may not conduct or sponsor, and, notwithstanding any other provision of law, a person is not required to respond to, an information collection unless the information collection displays a valid control number assigned by OMB.

As part of its continuing effort to reduce paperwork and respondent burden, the CFPB conducted a preclearance consultation program to provide the general public and Federal agencies with an opportunity to comment on the information collection requirements in

[224] SBREFA Panel Report at 40.

[225] Fed. Rsrv. Banks, *2023 Report on Employer Firms: Findings from the 2022 Small Business Credit Survey* (Mar. 2023), https://doi.org/10.55350/sbcs-20230308.

[226] 44 U.S.C. 3501 *et seq.*

accordance with the PRA. This helps ensure that the public understands the CFPB's requirements or instructions, respondents can provide the requested data in the desired format, reporting burden (time and financial resources) is minimized, information collection instruments are clearly understood, and the CFPB can properly assess the impact of information collection requirements on respondents.

The rule amends and adds to 12 CFR part 1033 and amends 12 CFR part 1001. The rule contains seven new information collection requirements.

1. Obligation to make covered data available (§ 1033.201), including general requirements (§ 1033.301) and requirements applicable to developer interface (§ 1033.311).

2. Information about the data provider (§ 1033.341).

3. Policies and procedures for data providers (§ 1033.351).

4. Third party authorization; general (§ 1033.401), including the authorization disclosure (§ 1033.411).

5. Third party obligations (§ 1033.421).

6. Use of data aggregator (§ 1033.431).

7. Policies and procedures for third party record retention (§ 1033.441).

The information collection requirements in this final rule are mandatory.

The collections of information contained in this rule, and identified as such, have been submitted to OMB for review under section 3507(d) of the PRA. A complete description of the information collection requirements (including the burden estimate methods) is provided in the information collection request (ICR) that the CFPB has submitted to OMB under the requirements of the PRA. The ICR submitted to OMB requesting approval under the PRA for the

information collection requirements contained herein is available at *www.regulations.gov* as well as on OMB's public-facing docket at *www.reginfo.gov*.

Title of Collection: 12 CFR part 1033.

OMB Control Number: 3170–XXXX.

Type of Review: New collection.

Affected Public: Private sector.

Estimated Number of Respondents: 10,285.

Estimated Total Annual Burden Hours: 1,435,650 annually and 5,664,085 one-time.

The CFPB will publish a separate *Federal Register* notice once OMB concludes its review announcing OMB approval of the information collections contained in this final rule.

In the proposal, the CFPB invited comments on: (1) Whether the collection of information is necessary for the proper performance of the functions of the CFPB, including whether the information will have practical utility; (2) the accuracy of the CFPB's estimate of the burden of the collection of information, including the validity of the methods and the assumptions used; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or other forms of information technology.

An industry association representing nondepositories commented that the PRA analysis in the proposal underestimated the burden of the information collection, particularly the costs estimated for policies and procedures for data providers and third party record retention, and the costs for data providers' obligations to make data available to third parties. The commenter stated that the cost and burden of the information collection would exceed the CFPB's estimate

of 120 hours annually per entity and would be prohibitively expensive for smaller entities, and encouraged the CFPB to reconsider its estimate of the burden from the information collection.

As discussed in part VI.E.1, the CFPB has increased its estimates for the costs of developing policies and procedures for data providers; these costs are estimated to be between $23,500 and $51,200 per data provider. Regarding the estimated annual burden per entity of the information collection, the CFPB expects that most burdens related to record retention and making data available will be one-time costs to develop and implement compliant systems. This is reflected in the CFPB's estimate of larger one-time costs from the information collection as compared to annual costs. Comments related to the one-time and annual costs of record retention, making data available, and policies and procedures are discussed in part VI.E.1. The CFPB did not receive data or evidence that would allow it to further refine its estimates of per entity annual costs, but notes that the overall costs of the information collection have been reduced due to changes in the coverage of the final rule.

The other comments on the rule generally are summarized above.

IX. Congressional Review Act

Pursuant to the Congressional Review Act (5 U.S.C. 801 *et seq.*), the CFPB will submit a report containing this rule and other required information to the U.S. Senate, the U.S. House of Representatives, and the Comptroller General of the United States at least 60 days prior to the rule's published effective date. The Office of Information and Regulatory Affairs has designated this rule as a "major rule" as defined by 5 U.S.C. 804(2).

X. Severability

The CFPB intends that, if any provision of the final rule, or any application of a provision, is stayed or determined to be invalid, the remaining provisions or applications are severable and shall continue in effect.[227]

However, this is subject to the following significant exception. The CFPB considers data providers' obligations to provide data under 12 CFR part 1033 to authorized third parties to be inseparable from the protections the CFPB is establishing in subpart D to ensure that authorized third parties are acting on behalf of consumers. Accordingly, if any of the provisions in subpart D were stayed or determined to be invalid, the CFPB intends that subpart D, together with references to third parties and authorized third parties elsewhere in part 1033, shall not continue in effect. This would not affect direct access by consumers to covered data under the remainder of part 1033, and it would also not affect the definition of financial product or service under § 1001.2(b).

The CFPB did not receive any comments opposing its approach to severability.[228]

List of Subjects

12 CFR Part 1001

Consumer protection, Credit.

[227] As non-exhaustive examples to illustrate the above, the following are severable from the remainder of the rule: the applicability of the rule to any type of data provider; the applicability of the rule to any type of covered consumer financial product or service; the applicability of the rule to any type of covered data; the reference in any provision of the rule to consensus standards; the fee prohibition in § 1033.301(c); any of the requirements for a developer interface under § 1033.311; and the applicability of § 1001.2(b) to any activity. Moreover, part 1033 and § 1001.2(b) are each severable from the other.

[228] The CFPB notes that this severability clause is not codified but forms an operative part of the rule.

12 CFR Part 1033

Banks, banking, Consumer protection, Credit, Credit Unions, Electronic funds transfers, National banks, Privacy, Reporting and recordkeeping requirements, Savings associations, Voluntary standards.

Authority and Issuance

For the reasons set forth in the preamble, the CFPB amends 12 CFR parts 1001 and part 1033, as set forth below:

PART 1001—FINANCIAL PRODUCTS OR SERVICES

1. The authority citation for part 1001 continues to read as follows:

Authority: 12 U.S.C. 5481(15)(A)(xi); and 12 U.S.C. 5512(b)(1).

2. Amend § 1001.2 by revising paragraph (b) and adding reserved paragraph (c) to read as follows:

§ 1001.2 Definitions.

* * * * *

(b) Providing 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, where the financial data processing is not offered or provided by a person who, by operation of 12 U.S.C. 5481(15)(A)(vii)(I) or (II), is not a covered person.

(c) [Reserved].

3. Revise part 1033 to read as follows:

PART 1033—PERSONAL FINANCIAL DATA RIGHTS

SUBPART A—GENERAL

Sec.

SUBPART B—MAKING COVERED DATA AVAILABLE

SUBPART C—DATA PROVIDER INTERFACES; RESPONDING TO REQUESTS

SUBPART D—AUTHORIZED THIRD PARTIES

APPENDIX A TO PART 1033-PERSONAL FINANCIAL DATA RIGHTS RULE: HOW TO APPLY FOR RECOGNITION AS A STANDARD SETTER

Authority: 12 U.S.C. 5512; 12 U.S.C. 5514; 12 U.S.C. 5533.

SUBPART A—GENERAL

§ 1033.101 Authority, purpose, and organization.

(a) *Authority*. The regulation in this part is issued by the Consumer Financial Protection Bureau (CFPB) pursuant to the Consumer Financial Protection Act of 2010 (CFPA), Pub. L. 111-203, tit. X, 124 Stat. 1955.

(b) *Purpose*. This part implements the provisions of section 1033 of the CFPA by requiring data providers to make available to consumers and authorized third parties, upon

request, covered data in the data provider's control or possession concerning a covered consumer financial product or service, in an electronic form usable by consumers and authorized third parties; and by prescribing standards to promote the development and use of standardized formats for covered data, including through industry standards developed by standard-setting bodies recognized by the CFPB. This part also sets forth obligations of third parties that would access covered data on a consumer's behalf, including limitations on their collection, use, and retention of covered data.

(c) *Organization*. This part is divided into subparts as follows:

(1) Subpart A establishes the authority, purpose, organization, coverage of data providers, compliance dates, and definitions applicable to this part.

(2) Subpart B provides the general obligation of data providers to make covered data available upon the request of a consumer or authorized third party, including what types of information must be made available.

(3) Subpart C provides the requirements for data providers to establish and maintain interfaces to receive and respond to requests for covered data.

(4) Subpart D provides the obligations of third parties that would access covered data on behalf of a consumer.

(5) Appendix A provides instructions for how a standard-setting body would apply for CFPB recognition.

§ 1033.111 Coverage of data providers.

(a) *Coverage of data providers.* A data provider has obligations under this part if it controls or possesses covered data concerning a covered consumer financial product or service

that the consumer obtained from the data provider, subject to the exclusion in paragraph (d) of this section.

(b) *Definition of covered consumer financial product or service*. *Covered consumer financial product or service* means a consumer financial product or service, as defined in 12 U.S.C. 5481(5), that is:

(1) A *Regulation E account*, which means an account, as defined in Regulation E, 12 CFR 1005.2(b);

(2) A *Regulation Z credit card*, which means a credit card, as defined in Regulation Z, 12 CFR 1026.2(a)(15)(i); or

(3) Facilitation of payments from a Regulation E account or Regulation Z credit card, excluding products or services that merely facilitate first party payments. For purposes of this part, a first party payment is a transfer initiated by the payee or an agent acting on behalf of the underlying payee. First party payments include payments initiated by loan servicers.

(c) *Definition of data provider*. *Data provider* means a covered person, as defined in 12 U.S.C. 5481(6), that is:

(1) A *financial institution*, as defined in Regulation E, 12 CFR 1005.2(i);

(2) A *card issuer*, as defined in Regulation Z, 12 CFR 1026.2(a)(7); or

(3) Any other person that controls or possesses information concerning a covered consumer financial product or service that the consumer obtained from that person.

Example 1 to paragraph (c): A digital wallet provider is a data provider.

(d) *Coverage threshold—Certain depository institutions*. The requirements of subparts B and C do not apply to data providers defined under § 1033.111(c)(1) through (3) that are depository institutions that hold total assets equal to or less than the SBA size standard, as determined in accordance with this paragraph (d). If at any point a depository institution that held

total assets greater than that SBA size standard as of or at any point after **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]** subsequently holds total assets below that amount, the requirements of subparts B and C continue to apply.

(1) *Determining SBA size standard*. For purposes of paragraph (d) of this section, the SBA size standard is the SBA size standard for the data provider's appropriate NAICS code for commercial banking, credit unions, savings institutions and other depository credit intermediation, or credit card issuing, as codified in 13 CFR 121.201.

(2) *Calculating total assets*. For purposes of paragraph (d) of this section, total assets held by a depository institution are determined by averaging the assets reported on its own four preceding quarterly call report submissions to the Federal Financial Institutions Examination Council or National Credit Union Association, as applicable, or its submissions to the appropriate oversight body to the extent it does not submit such reports to the Federal Financial Examination Council or National Credit Union Administration.

(3) *Merger or acquisition—coverage of surviving depository institution when there are not four quarterly call report submissions*. After a merger or acquisition the surviving depository institution shall determine quarterly assets prior to the merger or acquisition by using the combined assets reported on the quarterly call report submissions by all predecessor depository institutions. The surviving depository institution shall determine quarterly assets after the merger or acquisition by using the assets reported on the quarterly call report submissions by the surviving depository institution. The surviving depository institution shall determine total assets by using the average of the quarterly assets for the four preceding quarters, whether the quarterly assets are the combined assets of the predecessor depository institutions or from the surviving depository institution.

§ 1033.121 Compliance dates.

(a) *Determining assets and revenue for purposes of initial compliance dates*. A data provider's compliance date in paragraph (b) of this section is based on the calculation of total assets or total receipts, as appropriate, described in paragraphs (a)(1) and (2) of this section.

(1) With respect to a depository institution data provider, total assets are determined by averaging the assets reported on its 2023 third quarter, 2023 fourth quarter, 2024 first quarter, and 2024 second quarter call report submissions to the Federal Financial Institutions Examination Council or National Credit Union Administration, as applicable, or its submissions to the appropriate oversight body to the extent it does not submit such reports to the Federal Financial Examination Council or National Credit Union Administration. If, as a result of a merger or acquisition, a depository institution data provider does not have the named four quarterly call report submissions, the depository institution data provider shall use the process set out in § 1033.111(d)(3) to determine total assets for the time period named in this paragraph (a)(1).

(2) With respect to a nondepository institution data provider, total receipts are calculated based on the SBA definition of receipts, as codified in 13 CFR 121.104(a).

(b) *Initial compliance dates*. A data provider defined under § 1033.111(c)(1) through (3) must comply with the requirements in subparts B and C beginning on:

(1) April 1, 2026, for depository institution data providers that hold at least $250 billion in total assets and nondepository institution data providers that generated at least $10 billion in total receipts in either calendar year 2023 or calendar year 2024.

(2) April 1, 2027, for data providers that are:

(i) Depository institutions that hold at least $10 billion in total assets but less than $250 billion in total assets; or

(ii) Nondepository institutions that did not generate $10 billion or more in total receipts in both calendar year 2023 and calendar year 2024.

(3) April 1, 2028, for depository institution data providers that hold at least $3 billion in total assets but less than $10 billion in total assets.

(4) April 1, 2029, for depository institution data providers that hold at least $1.5 billion in total assets but less than $3 billion in total assets.

(5) April 1, 2030, for depository institution data providers that hold less than $1.5 billion in total assets but more than $850 million in total assets.

(c) *Compliance dates for depository institution data providers that subsequently cross coverage threshold*. A depository institution data provider under § 1033.111(c)(1) through (3) that has total assets as calculated in § 1033.111(d)(2) equal to or less than the SBA size standard as determined in accordance with § 1033.111(d)(1), but that subsequently holds total assets that exceed that SBA size standard, as measured in § 1033.111(d)(2), must comply with the requirements in subparts B and C within a reasonable amount of time after exceeding the size standard, not to exceed five years.

§ 1033.131 Definitions.

For purposes of this part, the following definitions apply:

Authorized third party means a third party that has complied with the authorization procedures described in § 1033.401.

Card issuer is defined at § 1033.111(c)(2).

Consensus standard means a standard that is adopted by a recognized standard setter and that continues to be maintained by that recognized standard setter.

Consumer means a natural person. Trusts established for tax or estate planning purposes are considered natural persons for purposes of this definition. *Consumer* also includes guardians, trustees, custodians, or other similar natural persons acting on behalf of a consumer pursuant to State law.

Consumer interface means 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.

Covered consumer financial product or service is defined at § 1033.111(b).

Covered data is defined at § 1033.211.

Data aggregator means a person that is retained by and provides services to the authorized third party to enable access to covered data.

Data provider is defined at § 1033.111(c).

Depository institution means any depository institution as defined by the Federal Deposit Insurance Act, 12 U.S.C. 1813(c)(1), or any credit union as defined by 12 CFR 700.2.

Developer interface means 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.

Financial institution is defined at § 1033.111(c)(1).

Recognized standard setter means a standard-setting body that has been recognized by the CFPB under § 1033.141.

Regulation E account is defined at § 1033.111(b)(1).

Regulation Z credit card is defined at § 1033.111(b)(2).

Third party means any person that is not the consumer about whom the covered data pertains or the data provider that controls or possesses the consumer's covered data.

§ 1033.141 Standard-setting bodies.

(a) *Recognition of a standard-setting body*. A standard-setting body may request CFPB recognition. Recognition will last up to five years, absent revocation. The CFPB will not recognize a standard-setting body unless it demonstrates that it satisfies the following attributes:

(1) *Openness:* The sources, procedures, and processes used are open to all interested parties, including: consumer and other public interest groups with expertise in consumer protection, financial services, community development, fair lending, and civil rights; authorized third parties; data providers; data recipients; data aggregators and other providers of services to authorized third parties; and relevant trade associations. Parties can meaningfully participate in standards development on a non-discriminatory basis.

(2) *Balance:* The decision-making power is balanced across all interested parties, including consumer and other public interest groups, and is reflected at all levels of the standard-setting body. There is meaningful representation for large and small commercial entities within these categories. No single interest or set of interests dominates decision-making. Achieving balance requires recognition that, even when a participant may play multiple roles, such as data provider and authorized third party, the weight of that participant's commercial concerns may align primarily with one set of interests. The ownership of participants is considered in achieving balance.

(3) *Due process and appeals:* The standard-setting body uses documented and publicly available policies and procedures, and it provides adequate notice of meetings and standards

development, sufficient time to review drafts and prepare views and objections, access to views and objections of other participants, and a fair and impartial process for resolving conflicting views. An appeals process is available for the impartial handling of procedural appeals.

(4) *Consensus:* Standards development proceeds by consensus, which is defined as general agreement, though not necessarily unanimity. During the development of consensus, comments and objections are considered using fair, impartial, open, and transparent processes.

(5) *Transparency:* Procedures or processes for participating in standards development and for developing standards are transparent to participants and publicly available.

SUBPART B—MAKING COVERED DATA AVAILABLE

§ 1033.201 Availability and prohibition against evasion.

(a) *Obligation to make covered data available*—(1) *General*. A data provider must make available to a consumer and an authorized third party, upon request, 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, in an electronic form usable by consumers and authorized third parties.

(2) *Prohibition against evasion*. A data provider must not take any action:

(i) With the intent of evading the requirements of subparts B and C of this part;

(ii) That the data provider knows or should know is likely to render unusable the covered data that the data provider makes available; or

(iii) That the data provider knows or should know is likely to prevent, interfere with, or materially discourage a consumer or authorized third party from accessing covered data consistent with this part.

(b) *Current data*. In complying with paragraph (a) of this section, a data provider must make available the most recently updated covered data that it has in its control or possession at the time of a request. A data provider must make available information concerning authorized but not yet settled transactions.

§ 1033.211 Covered data.

Covered data in this part means, as applicable:

(a) Transaction information, including historical transaction information in the control or possession of the data provider. A data provider is deemed to make available sufficient historical transaction information for purposes of § 1033.201(a)(1) if it makes available at least 24 months of such information.

Example 1 to paragraph (a): This category includes amount, transaction date, payment type, pending or authorized status, payee or merchant name, rewards credits, and fees or finance charges.

(b) Account balance information.

(c) Information to initiate payment to or from a Regulation E account directly or indirectly held by the data provider. This category includes an account and routing number that can be used to initiate an Automated Clearing House transaction.

(1) In complying with its obligation under § 1033.201(a)(1), a data provider is permitted to make available a tokenized account number instead of, or in addition to, a non-tokenized account number, as long as the tokenization is not used as a pretext to restrict competitive use of payment initiation information.

(2) This paragraph (c) does not apply to data providers who do not directly or indirectly hold the underlying Regulation E account. For example, a data provider that merely facilitates pass-through payments would not be required to make available account and routing number for the underlying Regulation E account.

(d) Terms and conditions. For purposes of this section, terms and conditions are limited to data in agreements evidencing the terms of the legal obligation between a data provider and a consumer for a covered consumer financial product or service, such data in the account opening agreement and any amendments or additions to that agreement, including pricing information.

Example 1 to paragraph (d): This category includes the applicable fee schedule, any annual percentage rate or annual percentage yield, credit limit, rewards program terms, whether a consumer has opted into overdraft coverage, and whether a consumer has entered into an arbitration agreement.

(e) Upcoming bill information.

Example 1 to paragraph (e): This category includes information about third party bill payments scheduled through the data provider and any upcoming payments due from the consumer to the data provider.

(f) Basic account verification information, which is limited to the name, address, email address, and phone number associated with the covered consumer financial product or service. If a data provider directly or indirectly holds a Regulation E or Regulation Z account belonging to the consumer, the data provider must also make available a truncated account number or other identifier for that account.

§ 1033.221 Exceptions.

A data provider is not required to make available the following covered data to a consumer or authorized third party:

(a) Any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors. Information does not qualify for this exception merely because it is an input to, or an output of, an algorithm, risk score, or predictor. For example, annual percentage rate and other pricing terms are sometimes determined by an internal algorithm or predictor but do not fall within this exception.

(b) Any information collected by the 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. Information collected for other purposes does not fall within this exception. For example, name and other basic account verification information do not fall within this exception.

(c) Any information required to be kept confidential by any other provision of law. Information does not qualify for this exception merely because the data provider must protect it for the consumer. For example, the data provider cannot restrict access to the consumer's own information merely because that information is subject to privacy protections.

(d) Any information that the data provider cannot retrieve in the ordinary course of its business with respect to that information.

SUBPART C—DATA PROVIDER INTERFACES; RESPONDING TO REQUESTS

§ 1033.301 General requirements.

(a) *Requirement to maintain interfaces*. A data provider subject to the requirements of this part must maintain a consumer interface and a developer interface. The consumer interface and the developer interface must satisfy the requirements set forth in this section. The developer interface must satisfy the additional requirements set forth in § 1033.311.

(b) *Machine-readable files upon request*. Upon request for covered data in a machine-readable file, and subject to paragraphs (b)(1) and (2) of this section, a data provider must make available to a consumer or an authorized third party covered data in a file that is machine-readable and that the consumer or authorized third party can retain and transfer for processing into a separate information system that is reasonably available to and in the control of the consumer or authorized third party.

(1) *Consumer interface*. With respect to covered data provided through its consumer interface, a data provider is not required to comply with:

(i) The requirements of this paragraph (b) for the covered data described in § 1033.211(c) (payment initiation information) and (f) (account verification information); and

(ii) The requirement of this paragraph (b) to provide in a file that is machine-readable the covered data described in § 1033.211(d) (terms and conditions).

(2) *Developer interface*. With respect to covered data provided through its developer interface, a data provider satisfies the requirements of this paragraph (b) if it makes available covered data in a form that satisfies the requirements of § 1033.311(b).

(c) *Fees prohibited*. A data provider must not impose any fees or charges on a consumer or an authorized third party in connection with:

(1) *Interfaces*. Establishing or maintaining the interfaces required by paragraph (a) of this section; or

(2) *Requests*. Receiving requests or making available covered data in response to requests as required by this part.

§ 1033.311 Requirements applicable to developer interface.

(a) *General.* A developer interface required by § 1033.301(a) must satisfy the requirements set forth in this section.

(b) *Standardized format*. The developer interface must make available covered data in a standardized and machine-readable format. Indicia that the format satisfies this requirement include that it conforms to a consensus standard.

(1) *Meaning of format*. For purposes of this section, *format* includes structures and definitions of covered data and requirements and protocols for communicating requests and responses for covered data.

(2) *Meaning of standardized*. For purposes of this section, *standardized* means conforms to a format widely used by other data providers and designed to be readily usable by authorized third parties.

(c) *Commercially reasonable performance.* A developer interface's performance must be commercially reasonable.

(1) *Response rate; quantitative minimum performance specification*. The performance of the interface cannot be commercially reasonable if it does not meet the following quantitative minimum performance specification regarding its response rate: The number of proper responses by the interface divided by the total number of requests for covered data to the interface must be equal to or greater than 99.5 percent in each calendar month. For purposes of this paragraph (c)(1), all of the following requirements apply:

(i) Any responses by and requests to the interface during scheduled downtime for the interface must be excluded respectively from the numerator and the denominator of the calculation.

(ii) In order for any downtime of the interface to qualify as scheduled downtime, the data provider must have provided reasonable notice of the downtime to all third parties to which the data provider has granted access to the interface. Indicia that the data provider's notice of the downtime may be reasonable include that the notice conforms to a consensus standard.

(iii) The total amount of scheduled downtime for the interface in a calendar month must be reasonable. Indicia that the total amount of scheduled downtime may be reasonable include that the amount conforms to a consensus standard.

(iv) A proper response is a response, other than any message provided during unscheduled downtime of the interface, that meets all of the following criteria:

(A) The response either fulfills the request or explains why the request was not fulfilled;

(B) The response is consistent with the reasonable written policies and procedures that the data provider establishes and maintains pursuant to § 1033.351(a); and

(C) The response is provided by the interface within a commercially reasonable amount of time. Indicia that a response is provided in a commercially reasonable amount of time include conformance to an applicable consensus standard.

(2) *Indicia of compliance*—(i) *Indicia*. Indicia that a developer interface's performance is commercially reasonable as required by paragraph (c) of this section include:

(A) Whether the interface's performance conforms to a consensus standard that is applicable to the data provider;

(B) How the interface's performance compares to the performance levels achieved by the developer interfaces of similarly situated data providers; and

(C) How the interface's performance compares to the performance levels achieved by the data provider's consumer interface.

(ii) *Performance specifications*. For each of the three indicia set forth in paragraph (c)(2)(i) of this section, relevant performance specifications include:

(A) The interface's response rate as defined in paragraphs (c)(1) through (c)(1)(iv) of this section;

(B) The interface's total amount of scheduled downtime;

(C) The amount of time in advance of any scheduled downtime by which notice of the downtime is provided;

(D) The interface's total amount of unscheduled downtime; and

(E) The interface's response time.

(d) *Access caps*. Except as otherwise permitted by §§ 1033.221, 1033.321, and 1033.331(b) and (c), a data provider must not unreasonably restrict the frequency with which it receives or responds to requests for covered data from an authorized third party through its developer interface. Any frequency restrictions must be applied in a manner that is non-discriminatory and consistent with the reasonable written policies and procedures that the data provider establishes and maintains pursuant to § 1033.351(a). Indicia that any frequency restrictions applied are reasonable include that they conform to a consensus standard.

(e) *Security specifications*—(1) *Access credentials*. A data provider must not allow a third party to access the data provider's developer interface by using any credentials that a consumer uses to access the consumer interface. A contract between a data provider and the data provider's service provider, pursuant to which the service provider establishes or maintains the data provider's developer interface, does not violate this paragraph if the contract provides that the service provider will make covered data available, in a form and manner that satisfies the requirements of this part, to authorized third parties through the developer interface by means of the service provider using a consumer's credentials to access the data from the data provider's consumer interface.

(2) *Security program.* (i) A data provider must apply to the developer interface an information security program that satisfies the applicable rules issued pursuant to section 501 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801; or

(ii) If the data provider is not subject to section 501 of the Gramm-Leach-Bliley Act, the data provider must apply to its developer interface the information security program required by the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 CFR part 314.

§ 1033.321 Interface access.

(a) *Denials related to risk management*. A data provider does not violate the general obligation in § 1033.201(a)(1) by denying a consumer or third party access to all elements of the interface described in § 1033.301(a) if:

(1) granting access would be inconsistent with policies and procedures reasonably designed to comply with:

(i) safety and soundness standards of a prudential regulator, as defined at 12 U.S.C. 5481(24), of the data provider;

(ii) information security standards required by section 501 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801; or

(iii) other applicable laws and regulations regarding risk management; and

(2) the denial is reasonable pursuant to paragraph (b).

(b) *Requirements for reasonable denials.* A denial is reasonable pursuant to paragraph (a)(2) of this section if it is:

(1) Directly related to a specific risk of which the data provider is aware, such as a failure of a third party to maintain adequate data security; and

(2) Applied in a consistent and non-discriminatory manner.

(c) *Indicia bearing on reasonable denials.* Indicia bearing on the reasonableness of a denial pursuant to paragraph (b) of this section include:

(1) Whether the denial adheres to a consensus standard related to risk management;

(2) Whether the denial proceeds from standardized risk management criteria that are available to the third party upon request; and

(3) Whether the third party has a certification or other identification of fitness to access covered data that is issued or recognized by a recognized standard setter or the CFPB.

(d) *Conditions sufficient to justify a denial*. Each of the following is a sufficient basis for denying access to a third party:

(1) The third party does not present any evidence that its information security practices are adequate to safeguard the covered data; or

(2) The third party does not make the following information available in both human-readable and machine-readable formats, and readily identifiable to members of the public, meaning the information must be at least as available as it would be on a public website:

(i) Its legal name and, if applicable, any assumed name it is using while doing business with the consumer;

(ii) A link to its website;

(iii) Its Legal Entity Identifier (LEI) that is issued by:

(A) A utility endorsed by the LEI Regulatory Oversight Committee, or

(B) A utility endorsed or otherwise governed by the Global LEI Foundation (or any successor thereof) after the Global LEI Foundation assumes operational governance of the global LEI system; and

(iv) Contact information a data provider can use to inquire about the third party's information security and compliance practices.

§ 1033.331 Responding to requests for information.

(a) *Responding to requests—access by consumers*. To comply with the requirements in § 1033.201(a)(1), upon request from a consumer, a data provider must make available covered data when it receives information sufficient to:

(1) Authenticate the consumer's identity; and

(2) Identify the scope of the data requested.

(b) *Responding to requests—access by third parties.* (1) To comply with the requirements in § 1033.201(a)(1), upon request from an authorized third party, a data provider must make available covered data when it receives information sufficient to:

(i) Authenticate the consumer's identity;

(ii) Authenticate the third party's identity;

(iii) Document the third party has followed the authorization procedures in § 1033.401; and

(iv) Identify the scope of the data requested.

(2) The data provider is permitted to confirm the scope of a third party's authorization to access the consumer's data by asking the consumer to confirm:

(i) The account(s) to which the third party is seeking access; and

(ii) The categories of covered data the third party is requesting to access, as disclosed by the third party pursuant to § 1033.411(b)(4).

Example 1 to paragraph (b): An authorized third party that a data provider has authenticated requests covered data on behalf of an authenticated consumer through the data provider's developer interface. The data provider asks the consumer to confirm the scope of the third party's authorization using a means of communication that the consumer is not accustomed to

using with the data provider and that the data provider knows or should know will take a long period of time to reach the consumer and allow the consumer to respond with the confirmation. As a result of the long wait time, the consumer cannot provide a timely confirmation, delaying the third party's access to the covered data. This data provider has violated the § 1033.201(a)(2) prohibition against evasion by taking an action that the data provider knows or should know is likely to interfere with an authorized third party's access to covered data.

(c) *Covered data not required to be made available.* A data provider is not required to make covered data available in response to a request when:

(1) The data are withheld because an exception described in § 1033.221 applies;

(2) The data are not in the data provider's control or possession, consistent with the requirement in § 1033.201(a)(1).

(3) The data provider's interface is not available when the data provider receives a request requiring a response under this section. However, the data provider is subject to the performance specifications in § 1033.311(c);

(4) The request is for access by a third party; and

(i) The consumer has revoked the third party's authorization pursuant to paragraph (e) of this section;

(ii) The data provider has received notice that the consumer has revoked the third party's authorization pursuant to § 1033.421(h)(2); or

(iii) The consumer has not provided a new authorization to the third party after the maximum duration period, as described in § 1033.421(b)(2).

(5) The data provider has not received information sufficient to satisfy the conditions in § 1033.331(a) or (b).

(d) *Jointly held accounts.* A data provider that receives a request for covered data from a consumer that jointly holds an account or from an authorized third party acting on behalf of such

a consumer must make available covered data to that consumer or authorized third party, subject to the other provisions of this section.

(e) *Method to revoke third party authorization to access covered data*. A data provider does not violate the general obligation in § 1033.201(a)(1) by making available to the consumer a reasonable method to revoke any third party's authorization to access all of the consumer's covered data, provided that such method does not violate § 1033.201(a)(2). Indicia that the data provider's revocation method is reasonable include its conformance to a consensus standard. A data provider that receives a revocation request from a consumer through a revocation method it makes available must revoke the authorized third party's access and notify the authorized third party of the request in a timely manner.

§ 1033.341 Information about the data provider.

(a) *Requirement to make information about the data provider readily identifiable*. A data provider must make the information described in paragraphs (b) through (d) of this section:

(1) Readily identifiable to members of the public, meaning the information must be at least as available as it would be on a public website; and

(2) Available in both human-readable and machine-readable formats.

(b) *Identifying information*. A data provider must disclose in the manner required by paragraph (a) of this section:

(1) Its legal name and, if applicable, any assumed name it is using while doing business with the consumer;

(2) A link to its website;

(3) Its LEI that is issued by:

(i) A utility endorsed by the LEI Regulatory Oversight Committee, or

(ii) A utility endorsed or otherwise governed by the Global LEI Foundation (or any successor thereof) after the Global LEI Foundation assumes operational governance of the global LEI system; and

(4) Contact information that enables a consumer or third party to receive answers to questions about accessing covered data under this part.

(c) *Developer interface documentation*. For its developer interface, a data provider must disclose in the manner required by paragraph (a) of this section documentation, including metadata describing all covered data and their corresponding data fields, and other documentation sufficient for a third party to access and use the interface. A data provider is not required to make publicly available information that would impede its ability to deny a third party access to its developer interface, consistent with § 1033.321. Indicia that documentation is sufficient for a third party to access and use a developer interface include conformance to a consensus standard. The documentation must:

(1) Be maintained and updated as reasonably necessary for third parties to access and use the interface in accordance with the terms to which data providers are subject under this part;

(2) Include how third parties can get technical support and report issues with the interface; and

(3) Be easy to understand and use, similar to data providers' documentation for other commercially available products.

(d) *Performance disclosure*. On or before the final day of each calendar month, a data provider must disclose in the manner required by paragraph (a) of this section the quantitative minimum performance specification for the response rate described in § 1033.311(c)(1)(i) through (iv) that the data provider's developer interface achieved in the previous calendar month.

The data provider's disclosure must include at least a rolling 13 months of the required monthly figure, except that the disclosure need not include the monthly figure for months prior to the compliance date applicable to the data provider. The data provider must disclose the metric as a percentage rounded to four decimal places, such as "99.9999 percent."

§ 1033.351 Policies and procedures.

(a) *Reasonable written policies and procedures*. A data provider must establish and maintain written policies and procedures that are reasonably designed to achieve the objectives set forth in subparts B and C of this part, including paragraphs (b) through (d) of this section. Policies and procedures must be appropriate to the size, nature, and complexity of the data provider's activities. A data provider has flexibility to design policies and procedures to avoid acting inconsistently with its other legal obligations, or in a way that could reasonably hinder enforcement against unlawful or potentially unlawful conduct. A data provider must periodically review the policies and procedures required by this section and update them as appropriate to ensure their continued effectiveness.

(b) *Policies and procedures for making covered data available*. The policies and procedures required by paragraph (a) of this section must be reasonably designed to ensure that:

(1) *Making available covered data.* A data provider creates a record of the data fields of covered data in the data provider's control or possession, what covered data are not made available through a consumer or developer interface pursuant to an exception in § 1033.221, and the reasons the exception applies. Indicia that a data provider's record of such data fields complies with the requirements of this paragraph include listing data fields that conform to those published by a consensus standard.

(2) *Denials of developer interface access.* When a data provider denies a third party access to a developer interface pursuant to § 1033.321, the data provider:

(i) Creates a record substantiating the basis for denial; and

(ii) Communicates in a timely manner to the third party, electronically or in writing, the reason(s) for the denial.

(3) *Denials of information requests.* When a data provider denies a request for information for a reason described in § 1033.331(c), to the extent the communication of the denial is not required to be standardized by § 1033.311(b), the data provider:

(i) Creates a record substantiating the basis for the denial; and

(ii) Communicates in a timely manner to the consumer or third party, electronically or in writing, the type(s) of information denied, if applicable, and the reason(s) for the denial.

(c)(1) *Policies and procedures for ensuring accuracy*. The policies and procedures required by paragraph (a) of this section must be reasonably designed to ensure that covered data are accurately made available through the data provider's developer interface.

(2) *Elements.* In developing its policies and procedures regarding accuracy, a data provider must consider, for example:

(i) Implementing the format requirements of § 1033.311(b); and

(ii) Addressing information provided by a consumer or a third party regarding inaccuracies in the covered data made available through its developer interface.

(3) *Indicia of compliance.* Indicia that a data provider's policies and procedures regarding accuracy are reasonable include whether the policies and procedures conform to a consensus standard regarding accuracy.

(d) *Policies and procedures for record retention*. The policies and procedures required by paragraph (a) of this section must be reasonably designed to ensure retention of records that are evidence of compliance with subparts B and C of this part.

(1) *Retention period*. Records that are evidence of a data provider's actions in response to a consumer's or third party's request for information or a third party's request to access a developer interface must be retained for at least three years after a data provider has responded to the request. All other records that are evidence of compliance with subparts B and C of this part must be retained for a reasonable period of time of at least three years from the date of the action required under subparts B and C of this part.

(2) *Certain records retained pursuant to policies and procedures.* Records retained pursuant to policies and procedures required under paragraph (a) of this section must include, without limitation:

(i) Records documenting requests for a third party's access to an interface, actions taken in response to such requests, and reasons for denying access, if applicable, for at least three years after the data provider has responded to the request;

(ii) Records providing evidence of fulfillment of requests for information, actions taken in response to such requests, and reasons for not making the information available, if applicable, for at least three years after the data provider has responded to the request;

(iii) Records documenting that the third party has followed the authorization procedures in § 1033.401 to access data on behalf of a consumer, for at least three years after such records are generated;

(iv) Records providing evidence of actions taken by a consumer and a data provider to revoke a third party's access pursuant to any revocation method made available by a data provider, for at least three years after the revocation;

(v) Records providing evidence of commercially reasonable performance described in § 1033.311(c)(2)(C)(ii), for at least three years after the period recorded;

(vi) Written policies and procedures required under § 1033.351 for three years from the time such material was last applicable; and

(vii) Disclosures required under § 1033.341, for three years from the time such material was disclosed to the public.

SUBPART D—AUTHORIZED THIRD PARTIES

§ 1033.401 Third party authorization; General.

To become an authorized third party, the third party must seek access to covered data from a data provider on behalf of a consumer to provide a product or service the consumer requested and:

(a) Provide the consumer with an authorization disclosure as described in § 1033.411;

(b) Provide a statement to the consumer in the authorization disclosure, as provided in § 1033.411(b)(5), certifying that the third party agrees to the obligations described in § 1033.421; and

(c) Obtain the consumer's express informed consent to access covered data on behalf of the consumer by obtaining an authorization disclosure that is signed by the consumer electronically or in writing.

§ 1033.411 Authorization disclosure.

(a) *In general*. To comply with § 1033.401(a), a third party must provide the consumer with an authorization disclosure electronically or in writing. The authorization disclosure must be clear, conspicuous, and segregated from other material. The names included in the authorization disclosure as required by paragraphs (b)(1) and (2) of this section and by § 1033.431(b) must be readily understandable to the consumer.

(b) *Content.* The authorization disclosure must include:

(1) The name of the third party that will be authorized to access covered data pursuant to the third party authorization procedures in § 1033.401.

(2) The name of the data provider that controls or possesses the covered data that the third party identified in paragraph (b)(1) of this section seeks to access on the consumer's behalf.

(3) A brief description of the product or service the consumer has requested from the third party identified in paragraph (b)(1) of this section and a statement that the third party will collect, use, and retain the consumer's data only as reasonably necessary to provide that product or service to the consumer.

(4) The categories of data that will be accessed. Categories must have a substantially similar level of specificity as the categories in § 1033.211.

(5) The certification statement described in § 1033.401(b).

(6) A brief description of the expected duration of data collection and a statement that collection will not last longer than one year after the consumer's most recent reauthorization.

(7) A description of the revocation method described in § 1033.421(h)(1).

(c) *Language access*—(1) *In general.* The authorization disclosure must be in the same language as the communication in which the authorization disclosure is conveyed to the

consumer. Any translation of the authorization disclosure provided to the consumer must be complete and accurate.

(2) *Additional languages.* If the authorization disclosure is in a language other than English, it must include a link to an English-language translation, and it is permitted to include links to translations in other languages. If the authorization disclosure is in English, it is permitted to include links to translations in other languages.

§ 1033.421 Third party obligations.

(a) *General limitation on collection, use, and retention of consumer data*—(1) *In general*. The third party will limit its collection, use, and retention of covered data to what is reasonably necessary to provide the consumer's requested product or service.

(2) *Specific purposes.* For purposes of paragraph (a)(1) of this section, the following are not part of, or reasonably necessary to provide, any other product or service:

(i) Targeted advertising;

(ii) Cross-selling of other products or services; or

(iii) The sale of covered data.

(b) *Collection of covered data*—(1) *In general*. Collection of covered data for purposes of paragraph (a) of this section includes the scope of covered data requested and the duration and frequency of collection of covered data.

(2) *Maximum duration*. In addition to the limitation described in paragraph (a) of this section, the third party will limit the duration of collection of covered data to a maximum period of one year after the consumer's most recent authorization.

(3) *Reauthorization after maximum duration*. To collect covered data beyond the one-year maximum period described in paragraph (b)(2) of this section, the third party will obtain a

new authorization from the consumer pursuant to § 1033.401 no later than the anniversary of the most recent authorization from the consumer. The third party is permitted to ask the consumer for a new authorization pursuant to § 1033.401 in a reasonable manner. Indicia that a new authorization request is reasonable include its conformance to a consensus standard.

(c) *Use of covered data*. Use of covered data for purposes of paragraph (a) of this section includes both the third party's own use of covered data and provision of covered data by that third party to other third parties. Examples of uses of covered data that are permitted under paragraph (a) of this section include:

(1) Uses that are specifically required under other provisions of law, including to comply with a properly authorized subpoena or summons or to respond to a judicial process or government regulatory authority;

(2) Uses that are reasonably necessary to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;

(3) Servicing or processing the product or service the consumer requested; and

(4) Uses that are reasonably necessary to improve the product or service the consumer requested.

(d) *Accuracy.* A third party will 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.

(1) *Flexibility.* A third party has flexibility to determine its policies and procedures in light of the size, nature, and complexity of its activities.

(2) *Periodic review.* A third party will periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness.

(3) *Elements*. In developing its policies and procedures regarding accuracy, a third party must consider, for example:

(i) Accepting covered data in a format required by § 1033.311(b); and

(ii) Addressing information provided by a consumer, data provider, or another third party regarding inaccuracies in the covered data.

(4) *Indicia of compliance*. Indicia that a third party's policies and procedures are reasonable include whether the policies and procedures conform to a consensus standard regarding accuracy.

(e) *Data security*. (1) A third party will apply to its systems for the collection, use, and retention of covered data an information security program that satisfies the applicable rules issued pursuant to section 501 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801); or

(2) If the third party is not subject to section 501 of the Gramm-Leach-Bliley Act, the third party will apply to its systems for the collection, use, and retention of covered data the information security program required by the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 CFR part 314.

(f) *Provision of covered data to other third parties*. Before providing covered data to another third party, subject to the limitation described in paragraphs (a) and (c) of this section, the third party will require the other third party by contract to comply with the third party obligations in paragraphs (a) through (f) of this section and the condition in paragraph (i) of this section upon receipt of the notice described in paragraph (h)(2) of this section.

(g) *Ensuring consumers are informed*. (1) Upon obtaining authorization to access covered data on the consumer's behalf, the third party will provide the consumer with a copy of the authorization disclosure that the consumer has signed electronically or in writing and that

reflects the date of the consumer's electronic or written signature. The third party will deliver that copy of the authorization disclosure to the consumer or make it available in a location that is readily accessible to the consumer, such as the third party's interface. If the third party makes the authorization disclosure available in such a location, the third party will ensure it is accessible to the consumer until the third party's access to the consumer's covered data terminates.

(2) The third party will provide contact information that enables a consumer to receive answers to questions about the third party's access to the consumer's covered data. The contact information must be readily identifiable to the consumer.

(3) The third party will establish and maintain reasonable written policies and procedures designed to ensure that the third party provides to the consumer, upon request, the information listed in this paragraph (g)(3) about the third party's access to the consumer's covered data. The third party has flexibility to determine its policies and procedures in light of the size, nature, and complexity of its activities, and the third party will periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness. The policies and procedures must be designed to ensure that the third party provides the following to the consumer, upon request:

(i) Categories of covered data collected;

(ii) Reasons for collecting the covered data;

(iii) Names of parties with which the covered data was shared. The names must be readily understandable to the consumer;

(iv) Reasons for sharing the covered data;

(v) Status of the third party's authorization;

(vi) How the consumer can revoke the third party's authorization to access the consumer's covered data and verification the third party has adhered to requests for revocation; and

(vii) A copy of any data aggregator certification statement that was provided to the consumer pursuant to § 1033.431(c)(2).

(h) *Revocation of third party authorization*—(1) *Provision of revocation method*. The third party will provide the consumer with a method to revoke the third party's authorization to access the consumer's covered data that is as easy to access and operate as the initial authorization. The third party will also ensure the consumer is not subject to costs or penalties for revoking the third party's authorization.

(2) *Notice of revocation*. The third party will notify the data provider, any data aggregator, and other third parties to whom it has provided the consumer's covered data when the third party receives a revocation request from the consumer.

(i) *Effect of maximum duration and revocation on collection, use, and retention*. If a consumer does not provide a new authorization as described in paragraph (b)(3) of this section, or if a third party receives a revocation request as described in paragraph (h)(1) of this section or notice of a consumer's revocation request as described in § 1033.331(e), a third party will:

(1) No longer collect covered data pursuant to the most recent authorization; and

(2) No longer 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 under paragraph (a) of this section.

§ 1033.431 Use of data aggregator.

(a) *Responsibility for authorization procedures when the third party will use a data aggregator.* A data aggregator is permitted to perform the authorization procedures described in § 1033.401 on behalf of the third party seeking authorization under § 1033.401 to access covered data. However, the third party seeking authorization remains responsible for compliance with the authorization procedures described in § 1033.401, and the data aggregator must comply with paragraph (c) of this section.

(b) *Disclosure of the name of the data aggregator.* The authorization disclosure must include the name of any data aggregator that will assist the third party seeking authorization under § 1033.401 with accessing covered data and a brief description of the services the data aggregator will provide.

(c) *Data aggregator certification.* When the third party seeking authorization under § 1033.401 will use a data aggregator to assist with accessing covered data on behalf of a consumer, the data aggregator must certify to the consumer that it agrees to the conditions on accessing the consumer's data in § 1033.421(a) through (f) and the condition in § 1033.421(i) upon receipt of the notice described in § 1033.421(h)(2) before accessing the consumer's data. For this requirement to be satisfied:

(1) The third party seeking authorization under § 1033.401 must include the data aggregator's certification in the authorization disclosure described in § 1033.411; or

(2) The data aggregator must provide its certification to the consumer, electronically or in writing, separate from the authorization disclosure. The certification must be in the same language as the authorization disclosure and must be clear, conspicuous, and segregated from other material. The name of any data aggregator in the certification must be readily

understandable to the consumer. If, after the consumer has completed the authorization procedures, the authorized third party retains a data aggregator to assist with accessing covered data on behalf of the consumer, this data aggregator must provide its certification in accordance with this paragraph (c)(2).

§ 1033.441 Policies and procedures for third party record retention.

(a) *General requirement.* A third party that is a covered person or service provider, as defined in 12 U.S.C. 5481(6) and (26), must establish and maintain written policies and procedures that are reasonably designed to ensure retention of records that are evidence of compliance with the requirements of subpart D.

(b) *Retention period.* Records required under paragraph (a) of this section must be retained for a reasonable period of time, not less than three years after a third party obtains the consumer's most recent authorization under § 1033.401(a).

(c) *Flexibility.* A third party covered under paragraph (a) of this section has flexibility to determine its policies and procedures in light of the size, nature, and complexity of its activities.

(d) *Periodic review.* A third party covered under paragraph (a) of this section must periodically review its policies and procedures and update them as appropriate to ensure their continued effectiveness to evidence compliance with the requirements of subpart D.

(e) *Certain records retained pursuant to policies and procedures.* Records retained pursuant to policies and procedures required under this section must include, without limitation:

(1) A copy of the authorization disclosure that is signed by the consumer electronically or in writing and reflects the date of the consumer's signature and a record of actions taken by the consumer, including actions taken through a data provider or another third party, to revoke the third party's authorization; and

(2) With respect to a data aggregator covered under paragraph (a) of this section, a copy of any data aggregator certification statement that was provided to the consumer pursuant to § 1033.431(c)(2).

APPENDIX A TO PART 1033-PERSONAL FINANCIAL DATA RIGHTS RULE: HOW TO APPLY FOR RECOGNITION AS A STANDARD SETTER

If you want the CFPB to designate your organization as a recognized standard setter, you should follow the steps described below.

We may amend this process from time to time.

STEP ONE: REQUESTING RECOGNITION

Submit a written request for recognition.[1]

This should include key contact information, evidence of your organization's policies and practices,[2] and an explanation of how your organization satisfies each of the requirements in the Personal Financial Data Rights rule to be a recognized standard setter.[3] Your request should also describe how current and/or anticipated standards issued by your organization relate to open banking.

In advance of filing your request, you can seek a pre-filing meeting with us. We can walk you through the application process and help you make a complete submission.

Send formal submissions, as well as requests for pre-filing meetings, to: openbankingstandards@cfpb.gov.

---

[1] Sensitive personal information should not be provided.

[2] Evidence may include (but is not limited to) charters, bylaws, policies, procedures, fee schedules, meeting minutes, membership lists, financial statements/disclosures, publicly available materials, and issued standards.

[3] Relevant legal requirements are described at 12 CFR 1033.141. When explaining how your organization meets these requirements, you should reference relevant elements of the evidence you submit in support of your application.

STEP TWO: ADDITIONAL INFORMATION AND PUBLIC COMMENT

After reviewing your submission, we may request additional information to ensure that your application is complete.

We may publish your application.

We may also seek public input on your application and invite your responses to any information we receive on that basis.

STEP THREE: OUR REVIEW

When reviewing your application, we consider whether your policies and practices meet all the requirements for recognition. We also evaluate whether your application is accurate and complete.

We prioritize and review applications based on the extent to which recognizing your organization helps us to implement open banking.[4]

STEP FOUR: APPLICATION DECISION

CFPB recognition will be publicly disclosed on our website, along with the applicable terms and conditions of such recognition, such as its duration.

If the CFPB declines to recognize your organization, we will notify you.

You may withdraw your application at any time or for any reason.

If we determine that your organization is close to meeting, but does not yet meet, the requirements for CFPB recognition, we may ask you to provide a written plan specifying how and when you will take the steps required for full recognition. If that plan is satisfactory, we may state on our website that your organization has received contingent recognition. Once you

[4] Section 1033 of the Consumer Financial Protection Act, 12 U.S.C. 5533, describes the CFPB's role in implementing open banking.

provide us with evidence that you have successfully executed on that plan (or otherwise addressed the relevant contingences), the CFPB may extend full recognition.

STEP FIVE: RECOGNITION

There are several points to keep in mind about recognition.

As a recognized standard setter, you agree that the CFPB may monitor your organization and that you will provide information that we request.

You must also provide us, within 10 days, written explanation of any material change to information that was submitted with your application or during recognition, as well as any reason your organization may no longer meet underlying requirements for recognition.

In addition, you must meet any other specified terms and conditions of your recognition, which may include our reserving the right to observe or participate in standard setting.

If your recognition is set to expire, you can apply for re-recognition by re-starting at Step One at least 180 days before expiration. We may temporarily extend your recognition while we consider your request for re-recognition.

We may modify or revoke your recognition. The CFPB expects to notify you of the reasons it intends to revoke or modify recognition, and to provide your organization with an opportunity to address the CFPB's concerns.

Rohit Chopra,

Director, Consumer Financial Protection Bureau.